

simple + secure

SafeGuard Enterprise
Installationsanleitung

Produktversion: 5.60
Stand: April 2011



Inhalt

1 SafeGuard Enterprise Überblick

SafeGuard Enterprise ist eine umfassende, modular aufgebaute Datensicherheitslösung, die Informationen und Informationsaustausch auf Servern, PCs und mobilen Endgeräten durch ein richtlinienbasiertes Verschlüsselungskonzept zuverlässig schützt.

Die zentrale Verwaltung wird im SafeGuard Management Center durchgeführt. Sicherheitsrichtlinien, Schlüssel und Zertifikate, Smartcards und Token können über ein rollenbasiertes Administrationskonzept übersichtlich verwaltet werden. Ausführliche Protokollierung und Reportfunktionen gewährleisten stets den Überblick über alle Ereignisse.

Auf Benutzerseite sind Datenverschlüsselung und Schutz vor Angreifern die primären Sicherheitsfunktionen von SafeGuard Enterprise. SafeGuard Enterprise fügt sich dabei nahtlos in die gewohnte Benutzerumgebung ein und lässt sich leicht und intuitiv bedienen. Die SafeGuard-eigene Authentisierung, die Power-on Authentication (POA), sorgt für den nötigen Zugriffsschutz und bietet komfortable Unterstützung bei der Wiederherstellung von Anmeldeinformationen.

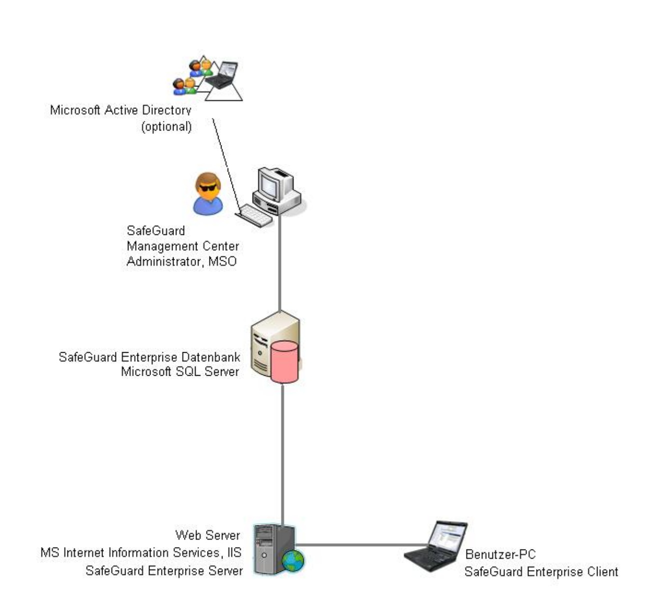
Hinweis: Nutzen Sie auch die Möglichkeit, SafeGuard Enterprise über Video-Tutorials kennenzulernen. Sie finden die Video-Tutorials in der Produktlieferung unter Tutorials. Sie zeigen die Installation von SafeGuard Enterprise und stellen die Arbeit mit dem SafeGuard Management Center vor.

2 SafeGuard Enterprise Komponenten

In diesem Kapitel lernen Sie die Komponenten von SafeGuard Enterprise und das Zusammenspiel zwischen den einzelnen Komponenten kennen.

Eine oder mehrere Microsoft SQL Datenbanken sammeln Informationen über die Endpoint-Computer im Firmennetzwerk. Der Administrator, bei SafeGuard Enterprise heißt er Haupt-Sicherheitsbeauftragter oder Master Security Officer (MSO), nutzt das SafeGuard Management Center, um die Datenbankinhalte zu steuern und neue Sicherheitsrichtlinien (Policies) zu erstellen.

Die PCs/Notebooks der Benutzer lesen die Richtlinien aus der Datenbank und berichten die erfolgreiche Ausführung an die Datenbank. Die Kommunikation zwischen Datenbank und Endpoint-Computern übernimmt dabei ein Internet Information Services (IIS) basierter Webserver, auf dem der SafeGuard Enterprise Server eingerichtet ist.



Die folgende Tabelle beschreibt die einzelnen Komponenten:

Komponente	Beschreibung
SafeGuard Enterprise Datenbank(en) basierend auf Microsoft SQL Server Datenbank	Die SafeGuard Enterprise Datenbank(en) enthält/enthalten alle relevanten Daten wie Schlüssel/Zertifikate, Informationen zu Benutzern & Computern, Ereignisse und die Richtlinieneinstellungen. Zugriff auf die Datenbank(en) benötigt der SafeGuard Enterprise Server und ein einziger Sicherheitsbeauftragter des SafeGuard Management Centers, meist der Haupt-Sicherheitsbeauftragte (MSO). Die Erzeugung und Konfiguration der SafeGuard Enterprise Datenbank(en) kann über einen Assistenten oder über Skripte erfolgen.

Komponente	Beschreibung
SafeGuard Enterprise Server auf IIS basiertem Webserver	Microsoft Internet Information Services (ISS) mit .NET Framework 3.5 SP 1 und ASP.NET 2.0. Der für SafeGuard Enterprise eingesetzte Webserver muss auf Internet Information Services (IIS) basieren. Wir empfehlen den Einsatz eines dedizierten IIS Servers für SafeGuard Enterprise Server. Es ist möglich, den IIS Server zu clustern.
	Der SafeGuard Enterprise Server ist die Schnittstelle zwischen Datenbank und SafeGuard Enterprise Endpoint-Computern. Der SafeGuard Enterprise Server sendet auf Anfrage SafeGuard Enterprise Richtlinieneinstellungen an die Endpoint-Computer. Er benötigt Zugriff auf die Datenbank. Er läuft als Anwendung auf einem Microsoft Internet Information Services (IIS) basierten Webserver.
SafeGuard Management Center mit .NET Framework 3.0 SP 1, ASP.Net 2.0 auf Administrator-Computer	Zentrales Management-Werkzeug für durch SafeGuard Enterprise geschützte Computer zur Verwaltung von Schlüsseln und Zertifikaten, Benutzern & Computern, sowie zur Erstellung von SafeGuard Enterprise Richtlinien. Das SafeGuard Management Center kommuniziert mit der SafeGuard Enterprise Datenbank.
Verzeichnisdienste (optional)	Import eines Active Directory. Es enthält die Organisationsstruktur des Unternehmens mit Benutzern und Computern.
SafeGuard Enterprise Client auf Endpoint-Computern	Client-Software zur Authentisierung und Datenverschlüsselung auf Endpoint-Computern. Der SafeGuard Enterprise Client (managed) kommuniziert mit dem SafeGuard Enterprise Server. Darüber hinaus lassen sich auch Standalone-Computer, Sophos SafeGuard Clients (standalone), die nie eine Verbindung zum SafeGuard Enterprise Server haben, mit SafeGuard Enterprise schützen.

3 Erste Schritte

Dieses Kapitel erklärt die notwendigen Vorbereitungsmaßnahmen für eine erfolgreiche Installation von SafeGuard Enterprise.

- Erstinstallation: Ein Installations-Assistent vereinfacht die erstmalige Einrichtung der Management-Komponenten einschließlich Standardrichtlinien. Um diesen Assistenten für neue SafeGuard Enterprise Installationen zu aktivieren, starten Sie **SGNInstallAdvisor.bat** aus dem Stammverzeichnis der Produktlieferung.
- Aktualisierung: Führen Sie die in dieser Hilfe beschriebenen Schritte durch.

3.1 Systemvoraussetzungen

Informationen zu Hardware- und Software-Anforderungen, Service Packs sowie Festplattenspeicherbedarf für Installation und effektiven Betrieb finden Sie auf der Systemanforderungen-Seite der Sophos Website (*http://www.sophos.de/products/enterprise/encryption/safeguard-enterprise/sysreqs.html*).

Für spezifische Anforderungen auf den Endpoint-Computern, *siehe Allgemeine Einschränkungen* (Seite 55).

3.2 Sprache der Benutzeroberfläche

Die Spracheinstellungen für die Installations- und Konfigurationsassistenten und die verschiedenen SafeGuard Enterprise Komponenten sind wie folgt:

3.2.1 Sprache während der Installation

Die Sprache der Installations- und Konfigurationsassistenten der verschiedenen Installationspakete wird automatisch an die Spracheinstellungen des Betriebssystems angepasst. Wenn die Betriebssystemsprache für diese Assistenten nicht verfügbar ist, wird standardmäßig Englisch benutzt.

3.2.2 Sprache des SafeGuard Management Center

So definieren Sie die Sprache des SafeGuard Management Center im SafeGuard Management Center:

1. Klicken Sie im **Extras** Menü auf **Optionen** und dann auf **Allgemein**. Klicken Sie auf **Benutzerdefinierte Sprache verwenden** und wählen Sie eine verfügbare Sprache aus. Die Sprachen Englisch, Deutsch, Französisch und Japanisch werden unterstützt.
2. Starten Sie das SafeGuard Management Center neu. Es wird in der ausgewählten Sprache angezeigt.

3.2.3 SafeGuard Enterprise Oberflächensprache auf Endpoint-Computern

Um die SafeGuard Enterprise Oberflächensprache auf dem Endpoint-Computer zu definieren, erstellen Sie eine Richtlinie vom Typ **Allgemeine Einstellungen** im SafeGuard Management Center und wählen Sie im Feld **Sprache am Client** unter **Anpassung** die gewünschte Sprache aus:

- Wenn die Sprache des Betriebssystems gewählt wird, richtet sich die Produktsprache nach der Spracheinstellung des Betriebssystems. Steht die entsprechende Betriebssystemsprache in SafeGuard Enterprise nicht zur Verfügung, wird standardmäßig die englische Version von SafeGuard Enterprise angezeigt.
- Wenn eine der zur Verfügung stehenden Sprachen gewählt wird, werden die SafeGuard Enterprise Produktanteile auf dem Endpoint-Computer in der ausgewählten Sprache angezeigt.

3.3 Zusammenspiel mit weiteren SafeGuard Produkten

Beachten Sie folgende Informationen zur Interaktion mit anderen SafeGuard Produkten.

3.3.1 Kompatibilität mit SafeGuard LAN Crypt

- SafeGuard LAN Crypt 3.7x und SafeGuard Enterprise 5.6x können zusammen auf einem Computer installiert werden und sind voll kompatibel.

  Hinweis:

  Wenn Sie SafeGuard Enterprise 5.6x über eine SafeGuard LAN Crypt Installation installieren, meldet das Installationsprogramm, dass die zu aktualisierende Komponente SGLC Profile Loader derzeit benutzt wird. Diese Meldung wird dadurch verursacht, dass SafeGuard LAN Crypt und SafeGuard Enterprise gemeinsame Komponenten benutzen. Die Meldung kann daher ignoriert werden. Die betroffenen Komponenten werden beim Neustart aktualisiert.

- SafeGuard LAN Crypt vor Version 3.7x und SafeGuard Enterprise 5.6x können nicht zusammen auf einem Computer installiert werden.

  Wenn Sie versuchen, SafeGuard Enterprise 5.6x auf einem Computer zu installieren, auf dem bereits SafeGuard LAN Crypt 3.6x oder eine ältere Version installiert ist, wird die Installation mit einer Fehlermeldung abgebrochen.

- SafeGuard LAN Crypt 3.7x und SafeGuard Enterprise vor Version 5.40 können nicht zusammen auf einem Computer installiert werden.

  Wenn Sie versuchen, SafeGuard LAN Crypt 3.7x auf einem Computer zu installieren, auf dem sich bereits SafeGuard Enterprise mit Versionen niedriger als 5.40 befindet, wird die Installation abgebrochen und eine entsprechende Fehlermeldung ausgegeben.

3.3.2 Kompatibilität mit SafeGuard PrivateCrypto und SafeGuard PrivateDisk

SafeGuard Enterprise 5.6x und die Standalone Produkte SafeGuard PrivateCrypto ab Version 2.30 sowie SafeGuard PrivateDisk ab Version 2.30 können gleichzeitig auf einem Computer installiert sein.

Sowohl SafeGuard PrivateCrypto als auch SafeGuard PrivateDisk können dann das SafeGuard Enterprise Schlüsselmanagement mit benutzen.

3.3.3 Kompatibilität mit SafeGuard Removable Media

Das Modul SafeGuard Data Exchange und SafeGuard Removable Media können nicht zusammen auf einem Computer installiert werden. Bevor Sie das Modul SafeGuard Data Exchange auf einem Computer installieren, prüfen Sie, ob SafeGuard Removable Media bereits installiert ist. In diesem Fall müssen Sie SafeGuard Removable Media deinstallieren, bevor Sie SafeGuard Data Exchange installieren.

Lokale Schlüssel, die vor dem Wechsel zu SafeGuard Data Exchange mit einer SafeGuard Removable Media Version vor 1.20 erzeugt wurden, können auf dem SafeGuard Enterprise Client benutzt werden. Sie werden jedoch nicht automatisch an die SafeGuard Enterprise Datenbank übertragen.

3.3.4 Kompatibilität mit SafeGuard Easy Version 4.x

SafeGuard Easy 4.x und SafeGuard Enterprise 5.6x können auf demselben Computer installiert werden, unter der Voraussetzung, dass das SafeGuard Device Encryption Module von SafeGuard Enterprise nicht installiert wird. Da beide Produkte eine eigene GINA (graphische Identifizierung und Authentisierung) installieren, funktioniert SafeGuard Enterprise nur korrekt, wenn die eigene GINA benutzt wird. Um eine korrekte Konfiguration zu gewährleisten, muss SafeGuard Easy 4.x ohne GINA-Unterstützung installiert werden (Option GINASYS = 0), bevor das relevante SafeGuard Enterprise Modul installiert wird. Wurde SafeGuard Easy 4.x mit GINA-Unterstützung installiert, muss die Software vor der Installation von SafeGuard Enterprise 5.6x entfernt werden.

Hinweis:

Wenn SafeGuard Easy 4.x und das SafeGuard Data Exchange Module auf einem Computer installiert sind, funktionieren die SafeGuard Easy GINA-Mechanismen (vor allem Windows Secure Autologon - SAL) nicht mehr. Um dies zu umgehen, muss SafeGuard Easy 4.x zuerst installiert werden und beide Produkte sollten nur zusammen deinstalliert werden (ohne Neustart), um GINA-Konflikte zu vermeiden.

3.4 Allgemeine Vorsichtsmaßnahmen

Die Computer, auf denen der SafeGuard Enterprise Server, die SafeGuard Enterprise Datenbank und das SafeGuard Management Center laufen, sollten vor unberechtigtem Zugriff geschützt werden. Hierzu sollten folgende praktische Maßnahmen durchgeführt werden:

- Setzen Sie nur vertrauenswürdige Administratoren ein oder wenden Sie das "Vieraugenprinzip" an.

- Schützen Sie die Computer vor elektronischen Angriffen (Firewalls, sichere Konfiguration, Virus-Scanner, regelmäßige Updates, starke Kennwörter usw.).
- Schützen Sie die Computer vor unberechtigtem physischen Zugriff (z. B. sicherer Standort in geschützten Räumlichkeiten).

3.5 Sichern von Transportverbindungen mit SSL

SafeGuard Enterprise unterstützt zur Erhöhung der Sicherheit die Verschlüsselung der Transportverbindungen zwischen den einzelnen Komponenten mit SSL.

- Die Verbindung zwischen dem Datenbankserver und dem Web Server sowie die Verbindung zwischen dem Datenbankserver und dem Computer, auf dem das SafeGuard Management Center installiert ist, kann mit SSL verschlüsselt werden.
- Die Verbindung zwischen dem SafeGuard Enterprise Server und dem SafeGuard Enterprise Client (managed) kann entweder mit SSL oder mit SafeGuard-spezifischer Verschlüsselung verschlüsselt werden. Der Vorteil bei SSL ist, dass es ein Standardprotokoll ist und eine schnellere Verbindung aufgebaut werden kann als mit der SafeGuard Transportverschlüsselung.

Hinweis:

Wir empfehlen dringend, SSL-verschlüsselte Kommunikation zwischen dem SafeGuard Enterprise Server und dem SafeGuard Enterprise Client zu verwenden, es sei denn, es handelt sich um Demo- oder Test-Installationen. Falls dies nicht möglich ist und die proprietäre SafeGuard-Verschlüsselung verwendet werden muss, so gilt die Obergrenze von 1000 Clients, die eine Verbindung mit einer Serverinstanz herstellen können.

SSL-Verschlüsselung kann für SafeGuard Enterprise während der Konfiguration der SafeGuard Enterprise Komponenten direkt nach der Installation eingestellt werden. Es kann jedoch ebenso gut nachträglich zu jedem beliebigen Zeitpunkt aktiviert werden. Eine Neuinstallation ist dazu nicht erforderlich. Es muss lediglich ein neues Konfigurationspaket erstellt und auf dem entsprechenden Server oder Client ausgeführt werden.

Bevor SSL für SafeGuard Enterprise aktiviert werden kann, muss eine funktionsfähige SSL-Umgebung eingerichtet werden.

3.5.1 Einrichten von SSL

Die folgenden allgemeinen Aufgaben müssen für die SSL-Einrichtung auf dem Web Server durchgeführt werden:

- Certificate Authority muss auf dem Server installiert sein, um die bei der SSL-Verschlüsselung verwendeten Zertifikate auszustellen.
- Ein Zertifikat muss ausgestellt werden und der IIS Server so konfiguriert werden, dass er SSL verwendet und auf das Zertifikat zeigt.
- Der Servername, den Sie bei der Konfiguration des SafeGuard Enterprise Servers angeben, muss identisch sein mit dem Servernamen, den Sie vorab im SSL-Zertifikat angegeben haben. Sonst können Client und Server nicht miteinander kommunizieren. Für jeden SafeGuard Enterprise Server wird ein separates SSL-Zertifikat benötigt.

- Wenn Sie Network Load Balancer einsetzen, vergewissern Sie sich, dass der Portbereich den SSL-Port mit einschließt.

Weitere Informationen erhalten Sie von unserem technischen Support oder hier:

- *http://msdn2.microsoft.com/en-us/library/ms998300.aspx*
- *http://support.microsoft.com/default.aspx?scid=kb;en-us;316898*
- *https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx*

3.5.2 Aktivieren der SSL-Verschlüsselung in SafeGuard Enterprise

So aktivieren Sie die SSL-Verschlüsselung in SafeGuard Enterprise:

- Verbindung zwischen Web Server und Datenbankserver:

  Aktivieren Sie SSL-Verschlüsselung während der Registrierung des SafeGuard Enterprise Servers im SafeGuard Management Center Konfigurationspakete-Werkzeug. Für weitere Informationen, *siehe Konfigurieren der Datenbankserver-Verbindung* (Seite 35) oder siehe: *http://www.sophos.de/support/knowledgebase/article/109012.html*.

- Für die Verbindung zwischen Datenbankserver und SafeGuard Management Center

  Aktivieren Sie die SSL-Verschlüsselung im SafeGuard Management Center Konfigurationsassistenten, *siehe Konfigurieren der Datenbankserver-Verbindung* (Seite 35).

- Verbindung zwischen SafeGuard Enterprise Server und durch SafeGuard Enterprise geschützte Computer

  Aktivieren Sie SSL-Verschlüsselung beim Erzeugen des Konfigurationspakets für den SafeGuard Enterprise Client (managed) im SafeGuard Management Center Konfigurationspakete-Werkzeug, *siehe Erstellen eines Konfigurationspakets für SafeGuard Enterprise Client (managed)* (Seite 60).

3.6 Installationsschritte für SafeGuard Enterprise

Um SafeGuard Enterprise zu installieren, führen Sie die beschriebenen Installationsschritte durch.

Alle SafeGuard Enterprise Installationskomponenten (.msi-Pakete) finden Sie in der Produktlieferung.

Hinweis:

Für die meisten Client-Installationspakete sind 64-Bit-Varianten für Windows 7 64-Bit und Windows Vista 64-Bit verfügbar (<Paketname>_64.msi). Wenn das Betriebssystem des Endpoint-Computers Windows 7 64-Bit oder Windows Vista 64-Bit ist, können Sie die 64-Bit-Variante der "Client" .msi-Pakete installieren.

Nr.	Schritt	Installation/Konfiguration
1	Vorbereiten der Installationen.	

Nr.	Schritt	Installation/Konfiguration
SafeGuard Enterprise Server		
2	Internet Information Services (IIS) mit .NET Framework 3.5 und ASP.NET 2.0 einrichten	
3	Zusätzliche Konfiguration für SSL.	
4	SafeGuard Enterprise Server auf dem IIS Server installieren	SGNServer.msi
SafeGuard Enterprise Datenbank		
5	Authentisierung für den SafeGuard Enterprise Haupt-Sicherheitsbeauftragten einrichten. Das Benutzerkonto wird für Microsoft SQL Server eingerichtet.	
6 (optional)	SafeGuard Enterprise Datenbank(en) über Skripts erzeugen.	SQL-Skripts im Verzeichnis Tools der Produktlieferung
SafeGuard Management Center		
7	SafeGuard Management Center für die zentrale Administration (z. B. Domänen, Benutzer, Schlüsseln, Richtlinien usw.) einrichten	SGNManagementCenter.msi
8	Basiskonfiguration der Administration: Datenbankverbindungen konfigurieren, SafeGuard Enterprise Datenbank(en) und Haupt-Sicherheitsbeauftragten anlegen.	SafeGuard Management Center Konfigurationsassistent
9	SafeGuard Enterprise Server registrieren und konfigurieren: Server-Konfigurationspaket erzeugen und auf dem IIS Server installieren	Server-Konfigurationspaket: Konfigurationspakete-Funktion im SafeGuard Management Center.
10	Organisationsstruktur erstellen oder aus Active Directory importieren	SafeGuard Management Center
SafeGuard Enterprise Client		
11	Obligatorisches vorbereitendes Paket installieren, um die Endpoint-Computer für eine erfolgreiche Installation vorzubereiten.	SGxClientPreinstall.msi
12	Eines der beiden SafeGuard Enterprise Verschlüsselungssoftware-Pakete auf dem Endpoint-Computer installieren:	
	SafeGuard Device Encryption: ■ Volume-basierende Verschlüsselung ■ dateibasierende Verschlüsselung (SafeGuard Data Exchange)	SGNClient.msi SGNClient_x64.msi

Nr.	Schritt	Installation/Konfiguration
	Dieses Installationspaket gilt sowohl für SafeGuard Enterprise Clients (managed) als auch für Sophos SafeGuard Clients (standalone).	
	SafeGuard Data Exchange: ■ Dateibasierende Verschlüsselung ■ ohne Power-on Authentication Dieses Installationspaket gilt sowohl für SafeGuard Enterprise Clients (managed) als auch für Sophos SafeGuard Clients (standalone). Für die Unterstützung von BitLocker Device Encryption nicht verfügbar	SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi
13 (optional)	Installieren Sie zusätzlich SafeGuard Configuration Protection: Schnittstellenschutz und Management von Peripheriegeräten auf Endpoint-Computern. Dieses Installationspaket gilt nur für SafeGuard Enterprise Clients, für Sophos SafeGuard Clients (standalone) nicht verfügbar.	SGN_CP_Client.msi
14	Endpoint-Computer konfigurieren: Konfigurationspaket für Endpoint-Computer (managed oder standalone) erzeugen und auf dem Endpoint-Computer installieren.	Konfigurationspaket: Konfigurationspakete-Funktion im SafeGuard Management Center.

3.7 Installationsschritte für SafeGuard Enterprise Client auf mehreren Betriebssystemen (Runtime-System)

Der so genannte Runtime Client, ermöglicht das Booten von einem sekundären Boot-Laufwerk, wenn mehrere Betriebssysteme installiert sind und erlaubt den Zugriff auf diese Laufwerke, wenn diese durch eine SafeGuard Enterprise Installation verschlüsselt sind

Diese Lösung steht sowohl für SafeGuard Enterprise Clients (managed) als auch für Sophos SafeGuard Clients (standalone) zur Verfügung.

Hinweis:

SafeGuard Enterprise for Windows unterstützt keine Apple Hardware und kann nicht in einer Bootcamp-Umgebung installiert werden.

Es kann nur das SafeGuard Device Encryption Installationspaket verwendet werden. Wenn nur SafeGuard Data Exchange installiert ist, kann der Runtime Client nicht verwendet werden. Wenn das Betriebssystem des Endpoint-Computers Windows 7 64-Bit oder Windows Vista 64-Bit ist, können Sie die 64-Bit-Variante der "Client " .msi-Pakete installieren.

Um SafeGuard Enterprise auf mehreren Betriebssystemen zu installieren, führen Sie die folgenden Installationsschritte durch:

Nr.	Schritt	Beschreibung	Installation/Konfiguration
1	Runtime-System auf dem Endpoint-Computer einrichten	SafeGuard Client Runtimepaket auf dem/den sekundären Boot-Laufwerk(en) des Endpoint-Computers installieren.	SGNClientRuntime.msi SGNClientRuntime_x64.msi
2	SafeGuard Verschlüsselungssoftware auf den Endpoint-Computern installieren	Ausstatten der Endpoint-Computer mit notwendigen Voraussetzungen für die erfolgreiche Installation der Verschlüsselungssoftware (obligatorisch).	SGxClientPreinstall.msi
		SafeGuard Device Encryption Installationspaket auf dem primären Boot-Laufwerk des Endpoint-Computers installieren.	SGNClient.msi SGNClient_x64.msi
3	Endpoint-Computer konfigurieren	Konfigurationspaket für Endpoint-Computer (managed oder standalone) erzeugen und auf dem Endpoint-Computer installieren.	SGNClientConfig.msi Client-Konfigurationspaket im Konfigurationspakete-Werkzeug des SafeGuard Management Center erzeugen

3.8 Vorbereiten der Installation

Vor der Installation von SafeGuard Enterprise empfehlen wir folgende vorbereitende Maßnahmen:

- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.
- Schließen Sie alle geöffneten Applikationen.
- Überprüfen Sie die Systemanforderungen, *http://www.sophos.de/products/enterprise/encryption/safeguard-enterprise/sysreqs.html*.
- Lesen Sie die Release Notes.

Für Informationen zu den vorbereitenden Maßnahmen auf dem Endpoint-Computer, *siehe Vorbereiten der Verschlüsselung* (Seite 57).

3.8.1 Installer Download

1. Gehen Sie auf *https://secure.sophos.com/support/updates/*.
2. Geben Sie Ihren MySophos Benutzer und Ihr Kennwort ein.

3. Klicken Sie auf der Web-Seite für **Data Protection** Downloads auf **SafeGuard Enterprise** und laden Sie die SafeGuard Enterprise Installer sowie die Dokumentation herunter.
4. Legen Sie die Dateien an einem Speicherort ab, an dem Sie auf diese für die Installation Zugriff haben.

4 Einrichten des SafeGuard Enterprise Servers

Der SafeGuard Enterprise Server stellt die Schnittstelle zu den SafeGuard Enterprise Clients her. Er greift wie das SafeGuard Management Center auf die Datenbank zu. Er läuft als Applikation auf einem Web Server basierend auf Microsoft Internet Information Services (IIS).

Wir empfehlen den Einsatz eines dedizierten IIS für SafeGuard Enterprise Server. Dadurch wird die Performance verbessert. Außerdem verhindert dies, dass andere Anwendungen mit SafeGuard Enterprise in Konflikt geraten, z. B. wegen der verwendeten Version von ASP.NET.

Dieses Kapitel beschreibt, wie Sie SafeGuard Enterprise Server auf IIS installieren. Zuerst müssen Sie Microsoft Internet Information Services (IIS) installieren und konfigurieren.

4.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Sie benötigen Windows Administratorrechte.
- Microsoft Internet Information Services (IIS) muss verfügbar sein.

  IIS ist kostenlos verfügbar. Sie finden das Programm z. B. auf Ihrer Windows-DVD oder auf der Microsoft Website.
- Wenn Sie SSL als Transportverschlüsselung zwischen SafeGuard Enterprise Server und SafeGuard Enterprise Client verwenden, muss der IIS dafür eingerichtet werden, *siehe Sichern von Transportverbindungen mit SSL* (Seite 9).

  > Ein Zertifikat muss ausgestellt werden und der IIS Server so konfiguriert werden, dass er SSL verwendet und auf das Zertifikat zeigt.
  > Der Servername, den Sie bei der Konfiguration des SafeGuard Enterprise Servers angeben, muss identisch sein mit dem Servernamen, den Sie vorab im SSL-Zertifikat angegeben haben. Sonst können Client und Server nicht miteinander kommunizieren. Für jeden SafeGuard Enterprise Server wird ein separates SSL-Zertifikat benötigt.
  > Wenn Sie Network Load Balancer einsetzen, vergewissern Sie sich, dass der Portbereich den SSL-Port mit einschließt.

- .NET Framework 3.5 Service Pack 1 muss verfügbar sein.

  Sie finden das Programm in der SafeGuard Enterprise Produktlieferung.
- ASP.NET Version 2.0.50727 muss verfügbar sein.

  Sie finden das Programm z. B. auf Ihrer Windows-DVD. Je nach Windows-Version wird es bereits als Standard mit installiert. Sie können das Programm auch herunterladen: *http://www.asp.net/* . ASP.NET ist kostenlos verfügbar.

4.2 Installation und Konfiguration von Microsoft Internet Information Services (IIS)

Dieses Kapitel beschreibt, wie Sie Microsoft Internet Information Services (IIS) für den Betrieb mit SafeGuard Enterprise Server vorbereiten.

Die Einstellungen variieren je nach IIS-Version und Betriebssystemversion. Für folgende Kombinationen werden spezifische Setup-Informationen angegeben:

- IIS 6 auf Microsoft Windows Server 2003
- IIS 7 auf Microsoft Windows Server 2008

4.2.1 Installieren und Konfigurieren von IIS 6 auf Microsoft Windows Server 2003

IIS ist kostenlos verfügbar. Sie finden das Programm z. B. auf Ihrer Windows-DVD oder auf der Microsoft Website.

1. Klicken Sie im **Start** Menü auf **Systemsteuerung** und wählen Sie **Windows-Komponenten hinzufügen/entfernen**.
2. Klicken Sie in der **Komponenten** Liste auf **Application Server**.
3. Klicken Sie in **Application Server** auf **Details** und wählen Sie **Internet Information Services (IIS)**.
4. Wählen Sie außerdem **ASP.NET**.
5. Klicken Sie auf **OK**.

   IIS 6 wird mit einer Standardkonfiguration zum Hosten von ASP.NET installiert.

6. Überprüfen Sie mit http://< server name>, ob die Web-Seite korrekt angezeigt wird. Weitere Informationen finden Sie hier: *http://support.microsoft.com*.

4.2.1.1 Prüfen der .NET Framework Installation und Registrierung

.NET Framework Version 3.5 SP 1 ist erforderlich. Sie finden das Programm in der SafeGuard Enterprise Produktlieferung.

So überprüfen Sie, ob das Programm korrekt auf IIS 6 oder IIS 7 installiert ist:

1. Wählen Sie im **Start** Menü den Befehl **Ausführen...**.
2. Geben Sie folgendes Kommando ein: **Appwiz.cpl**. Alle auf dem Computer installierten Programme werden angezeigt.
3. Überprüfen Sie, ob .NET Framework Version 3.5 SP 1 angezeigt wird. Wird die Version nicht angezeigt, installieren Sie sie. Folgen Sie den Schritten im Installationsassistenten und bestätigen Sie alle Standardeinstellungen.
4. Um zu prüfen, ob die Installation korrekt registriert ist, wechseln Sie in C:\Windows\Microsoft.NET\Framework. Jede installierte Version muss als separater Ordner mit der Version als Ordnername sichtbar sein, "v3.5".

4.2.1.2 Prüfen der ASP.NET Registrierung bei IIS 6

ASP.NET Version 2.0.50727 ist erforderlich.

So überprüfen Sie, ob die korrekte ASP.NET Version installiert und bei IIS 6 registriert ist:

1. Öffnen Sie den **Internet Information Services Manager** auf dem IIS Server.
2. Klicken Sie im Navigationsbereich auf der rechten Seite unter **Internet Information Services** auf SGNSRV (**lokaler Computer**) und dann auf **Websites**.
3. Klicken Sie unter **Websites** mit der rechten Maustaste auf **Standard-Websites** und dann auf **Eigenschaften**. Wählen Sie die **ASP.NET** Registerkarte. Unter **ASP.NET Version** sollte Version 2.0.50727 angezeigt werden.
   - Wenn diese Version angezeigt wird, wählen Sie sie aus. Klicken Sie auf **Anwenden** und dann auf **OK**.
   - Wird die Version nicht angezeigt wird, geben Sie den Befehl

     aspnet_regiis.exe -lv auf der Kommandozeile ein, um sicherzustellen, dass die ASP Services in der Version 2.050727 installiert sind.
4. Um zu überprüfen, ob die korrekte Version installiert ist, geben Sie **aspnet_regiis.exe -lv** auf der Kommandozeile ein.

Als ASP.NET Version sollte 2.0.50727 angezeigt werden.

4.2.1.3 Konfigurieren von ASP.NET für IIS 6 auf Windows Server 2003 64 Bit

Wenn Sie IIS 6 verwenden und SafeGuard Enterprise Server auf Windows Server 2003 64 Bit installieren wollen, führen Sie die folgenden zusätzlichen Schritte durch:

1. Geben Sie folgenden Befehl ein: **cscript %SYSTEMDRIVE%\inetpub\adminscripts\adsutil.vbs SET W3SVC/AppPools/Enable32bitAppOnWin64 1**
2. Registrieren Sie die benötigte ASP.NET Version mit folgendem Kommando: **%SYSTEMROOT%\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -i**
3. Um die 32-Bit Version von ASP.Net 2.0.50727 zu aktivieren, öffnen Sie den **Internet Information Services Manager** auf dem IIS Server.
4. Klicken Sie im **IIS Manager** auf **Server** (**lokaler Computer**) und dann auf **Webdiensterweiterungen**.
5. Klicken Sie mit der rechten Maustaste auf **ASP.NET v2.0.50727** (**32 Bit**), klicken Sie auf **Eigenschaften** und setzen Sie den Status auf **Zugelassen**.
6. Klicken Sie auf **Anwenden** und dann auf **OK**.

4.2.1.4 Spezifisches SafeGuard Benutzerkonto für IIS 6

Während der Konfiguration von IIS 6 wird ein Benutzer angelegt, der sich anonym vom Client am SGNSRV-Bereich auf dem IIS anmeldet.

Wenn der SafeGuard Enterprise Server auf dem IIS Server installiert wird, wird der individualisierte Benutzer **IUSR_SafeGuard** angelegt. Mit **IUSR_SafeGuard** können Sie auch dann immer noch den anonymen Zugang zum SGNSRV-Bereich nutzen, wenn sich der IIS-Hostname ändert.

Bei IIS 6 ist der Standardbenutzername IUSR_MACHINENAME. Wenn der IIS-Hostname nach der Installation geändert wird, stimmt er nicht mehr mit dem Standardbenutzernamen überein und der anonyme Zugang schlägt fehl. Mit **IUSR_SafeGuard** haben Sie immer einen gültigen Anmeldenamen, auch wenn der IIS-Hostname geändert wird.

4.2.2 Installieren und Konfigurieren von IIS 7 auf Microsoft Windows Server 2008

IIS ist kostenlos verfügbar. Sie finden das Programm z. B. auf Ihrer Windows-DVD oder auf der Microsoft Website.

1. Klicken Sie im **Start** Menü auf **Alle Programme**, **Administration** und dann auf **Server-Manager**.
2. Scrollen Sie im **Server Manager** zur **Rollenübersicht** und klicken Sie auf **Rollen hinzufügen**.
3. Verifizieren Sie auf der **Vorbemerkungen** Seite des **Rollen hinzufügen** Assistenten Folgendes:
   - Das Administratorenkonto hat ein sicheres Kennwort.
   - Die Netzwerkeinstellungen, z. B. IP-Adressen, sind konfiguriert.
   - Die neuesten Windows-Sicherheits-Updates sind installiert.
4. Wählen Sie **Rollen auswählen** auf der rechten Seite und dann **Webserver (IIS)**. Klicken Sie auf der folgenden Seite auf **Erforderliche Features hinzufügen** Seite. **Webserver (IIS)** ist im Navigationsbereich des **Rollen hinzufügen** Assistenten aufgelistet.
5. Klicken Sie auf **Webserver (IIS)** und dann auf **Rollendienste**. Behalten Sie die Standard-Rollendienste bei.
6. Wählen Sie auf der rechten Seite zusätzlich Folgendes: **ASP.NET**, dadurch werden alle notwendigen untergeordneten Rollendienste ebenfalls ausgewählt. Wählen Sie dann **.NET Extensibility**, **ISAPI Extensions** und **ISAPI Filters**.
7. Wählen Sie **IIS Management Scripts and Tools**. Dies ist für die richtige IIS 7 Konfiguration erforderlich.
8. Klicken Sie auf **Weiter**, dann auf **Installieren** und dann auf **Schließen**.

   IIS 7 wird mit der Standardkonfiguration für das Hosten von ASP.Net auf Windows Server 2008 installiert.

9. Überprüfen Sie mit http://< server name>, ob die Web-Seite korrekt angezeigt wird. Weitere Informationen finden Sie hier: *http://support.microsoft.com*.

4.2.2.1 Prüfen der .NET Framework Registrierung bei IIS 7

.NET Framework Version 3.5 SP 1 ist erforderlich.

1. Um zu überprüfen, ob .NET Framework installiert und mit der korrekten Version registriert ist, *siehe Prüfen der .NET Framework Installation und Registrierung* (Seite 16).

4.2.2.2 Prüfen der ASP.NET Registrierung bei IIS 7

ASP.NET Version 2.0.50727 ist erforderlich.

1. Um zu überprüfen, ob ASP.NET installiert und mit der korrekten Version registriert ist, geben Sie das Kommando **aspnet_regiis.exe -lv** auf der Kommandozeile ein.

Als ASP.NET Version sollte 2.0.50727 angezeigt werden.

4.2.3 Aktivieren der Speicherwiederverwendung

Wir empfehlen, für IIS 6/IIS7 die Option **Arbeitsprozesse wieder verwenden** zu aktivieren.

1. Öffnen Sie den **Internet Information Services Manager** auf dem IIS Server.
2. Klicken Sie im **IIS Manager** auf **Server (lokaler Computer)**.
3. Klicken Sie mit der rechten Maustaste auf **Anwendungspools** und dann auf **Eigenschaften**.
4. Setzen Sie unter **Speicherwiederverwendung** folgende Werte:
   a) Maximaler virtueller Speicher = 500 MB
   b) Maximaler verwendeter Speicher = 192 MB
5. Klicken Sie auf **Anwenden** und dann auf **OK**.

Die Speicherwiederverwendung ist nun bei IIS 6/IIS 7 aktiviert.

4.3 Härten des IIS

Zur Erhöhung der Sicherheit im Intranet Ihres Unternehmens empfehlen wir, jeden IIS Server sowie die Anwendungen, die auf diesem Server laufen, durch spezifische Sicherheitseinstellungen zu schützen und ihn so zu „härten“.

Dieses Kapitel beschreibt, wie Sie den IIS Server für die Benutzung mit SafeGuard Enterprise so einrichten, dass er den Absicherungsempfehlungen von Microsoft entspricht. Sollten weitere Einstellungen, die nicht von Microsoft empfohlen oder in diesem Kapitel beschrieben werden, aktiviert werden, kann dies zu unerwünschten Ergebnissen führen.

Hinweis:

Detaillierte Informationen zur Absicherung von Web Servern finden Sie im Microsoft Solutions for Security and Compliance: Windows Server 2003 Security Guide, der auf der Microsoft Website kostenlos zum Download zur Verfügung steht.

Die Beschreibungen in diesem Kapitel basieren auf folgender Musterkonfiguration:

- Server 1:

  Microsoft Windows Server 2003 SP1
  SafeGuard Enterprise Server, aktuelle Version
  SafeGuard Management Center, aktuelle Version
  Microsoft SQL Server 2005 Express
  IIS mit minimalen Komponenten

- Server 2:

  Microsoft Windows Server 2003 SP1
  SafeGuard Enterprise Server, aktuelle Version
  Microsoft SQL Server 2005 Express
  IIS mit minimalen Komponenten

  Auf Server 2 läuft nur der SafeGuard Enterprise Server (IIS Server). Wenn Server 2 zusätzlich in Gebrauch ist, werden die für Server 1 aktivierten Dienste automatisch deaktiviert.

- Client:

  SafeGuard Enterprise Client
  SafeGuard Management Center, aktuelle Version

4.3.1 Nur notwendige IIS-Komponenten installieren

Stellen Sie sicher, dass nur notwendige IIS-Komponenten installiert werden. Dadurch reduziert sich das Risiko, dass der IIS Server angegriffen wird. Deaktivieren Sie alle unnötigen Einstellungen.

Der IIS Server läuft mit SafeGuard Enterprise Server mit den folgenden minimalen Komponenten:

- Gemeinsame Dateien
- Internetinformationsdienste-Manager (IIS-Manager)
- WWW-Publishingdienst

4.3.2 Nur notwendige Webdiensterweiterungen aktivieren

Stellen Sie sicher, dass nur notwendige Webdiensterweiterungen aktiviert werden. Dadurch reduziert sich das Risiko, dass der IIS Server angegriffen wird. Deaktivieren Sie alle unnötigen Einstellungen.

Die folgenden Einstellungen sind notwendig, damit der IIS Server mit dem SafeGuard Enterprise Server läuft:

Webdiensterweiterungen:

- ASP.NET v.1.1.4322 **Prohibited**
- ASP.NET v.2.50727 **Allowed**

4.3.3 Website-Inhalte auf eigener Partition

IIS speichert die Dateien für seine Default-Website in folgendem Ordner:

%systemroot%\inetpub\wwwroot

%systemroot% ist das Laufwerk, auf dem das Windows Server 2003 Betriebssystem installiert ist.

Verschieben Sie alle Dateien und Ordner für Websites und Applikationen auf eigene Partitionen, die vom Betriebssystem getrennt sind. Dies trägt zur Verhinderung von Angriffen bei, bei denen der Angreifer eine Anfrage nach einer Datei sendet, die sich außerhalb der Verzeichnisstruktur des IIS-Servers befindet.

Für die Musterkonfiguration können die Dateien und Ordner wie folgt verschoben werden:

- IIS Web-Dateien nach **E:\inetpub**
- SafeGuard Enterprise Server Web-Dateien nach **F:\mycompany.web**

Hinweis:

Nach dem Verschieben der Web-Dateien müssen Sie die Pfadinformationen im IIS-Manager entsprechend aktualisieren.

4.3.4 Einstellen von NTFS-Berechtigungen

Computer, auf denen Windows Server 2003 mit SP1 läuft, bestimmen anhand der NTFS-Dateisystemberechtigungen die Zugriffsrechte, die ein Benutzer oder ein Prozess an einer spezifischen Datei oder einem Ordner besitzt. Sie sollten daher NTFS-Berechtigungen zuweisen, um den Website-Zugriff bestimmten Benutzern auf dem IIS Server zu erlauben oder zu verweigern.

Für die Musterkonfiguration lauten die minimalen NTFS-Berechtigungen wie folgt:

Benutzer/Verzeichnis	NTFS-Berechtigungen für E:\inetpub	NTFS-Berechtigungen für F:\mycompany.web
Administratoren	Vollzugriff	Vollzugriff
System	Vollzugriff	Vollzugriff
Benutzer	Ausführen	Ausführen

Für „Benutzer“ können Sie ein anderes Konto oder eine andere Gruppe einstellen, unter der Voraussetzung, dass dies auf dem IIS Server zur Verfügung gestellt wird. In diesem Fall müssen Sie das Konto IUSR_SRVERNAME auf dem IIS Server entsprechend aktualisieren.

Die NTFS-Berechtigungen für Dateitypen lauten wie folgt:

Dateityp	Empfohlene NTF Berechtigungen
CGI Dateien (.exe, .dll, .cmd, .pl)	Administratoren (Vollzugriff) System (Vollzugriff) Jeder/Benutzer (Ausführen)
Skript-Dateien (.asp)	Administratoren (Vollzugriff) System (Vollzugriff) Jeder/Benutzer (Ausführen)

Dateityp	Empfohlene NTF Berechtigungen
Inklusive Dateien (.inc, .shtm, .shtml)	Administratoren (Vollzugriff) System (Vollzugriff) Jeder/Benutzer (Ausführen)
Statischer Content (.txt, .gif, .jpg, .htm, .html)	Administratoren (Vollzugriff) System (Vollzugriff) Jeder/Benutzer (Nur lesen)

4.3.5 Deaktivieren der integrierten Windows-Authentifizierung

Wir empfehlen, die integrierte Windows-Authentisierung in IIS zu deaktivieren, um so das Senden unnötiger Authentisierungsinformationen zu vermeiden.

1. Doppelklicken Sie im IIS-Manager auf den lokalen Computer, klicken Sie mit der rechten Maustaste auf den Ordner **Websites** und klicken Sie danach auf **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Verzeichnissicherheit** und danach im Bereich **Authentifizierung und Zugriffssteuerung** auf **Bearbeiten**.
3. Deaktivieren Sie unter **Authentifizierter Zugriff** das Kontrollkästchen **Integrierte Windows-Authentifizierung**.
4. Klicken Sie zweimal auf **OK**.

4.3.6 Einstellungen für den Anwendungspool "DefaultAppPool"

Die Einstellungen sind davon abhängig, wo sich der IIS Server befindet:

- Wenn sich der SQL Server auf dem gleichen Computer wie der IIS Server befindet, stellen Sie das eingebaute Local Service Benutzerkonto für "DefaultAppPool" ein. In der Musterkonfiguration gilt dies für Server 1.
- Wenn sich der SQL Server auf einem anderen Computer als der IIS Server befindet, stellen Sie das eingebaute Network Service Benutzerkonto für "DefaultAppPool" ein. In der Musterkonfiguration gilt dies für Server 2. Andernfalls schlägt die Synchronisierung mit dem Client fehl.

4.4 Installieren von SafeGuard Enterprise Server

Nachdem der IIS konfiguriert ist, können Sie SafeGuard Enterprise Server auf dem IIS Server installieren. Das Installationspaket **SGNServer.msi** finden Sie in der Produktlieferung.

1. Starten Sie **SGNServer.msi**.
2. Klicken Sie auf der **Willkommen** Seite auf **Weiter**.
3. Akzeptieren Sie die Lizenzvereinbarung.
4. Übernehmen Sie den Standardinstallationspfad.
5. Klicken Sie auf **Beenden**, um die Installation abzuschließen.

SafeGuard Enterprise Server ist installiert.

Hinweis:

Aus Performance-Gründen ist die Verkettung von protokollierten Ereignissen für die SafeGuard Enterprise Datenbank nach der Installation des SafeGuard Enterprise Servers standardmäßig deaktiviert. Ohne die Verkettung steht für die protokollierten Ereignisse jedoch kein Integritätsschutz zur Verfügung. Die Verkettung verknüpft alle Einträge in der Ereignistabelle miteinander, so dass die Entfernung eines Eintrags sichtbar wird und über eine Integritätsprüfung nachgewiesen werden kann. Um den Integritätsschutz zu nutzen, aktivieren Sie die Verkettung manuell. Weitere Informationen finden Sie in der Administrator-Hilfe im Kapitel *Berichte*.

5 Einrichten einer SafeGuard Enterprise Datenbank

SafeGuard Enterprise speichert alle relevanten Daten wie Schlüssel/Zertifikate, Informationen zu Benutzern & Computern, Ereignisse und die Richtlinieneinstellungen in einer Datenbank. Die SafeGuard Enterprise Datenbank basiert auf Microsoft SQL Server.

Eine Liste der derzeit unterstützten SQL Servertypen finden Sie in den *Systemanforderungen*.

Sie können die Datenbank entweder automatisch während der Erstkonfiguration im SafeGuard Management Center oder manuell mit den in Ihrer Produktlieferung verfügbaren SQL Skripten einrichten. Wählen Sie die geeignete Methode nach den Gegebenheiten in Ihrer Firmenumgebung. Für weitere Informationen, *siehe Datenbankzugriffsrechte* (Seite 25).

Zur Optimierung der Performance lässt sich die SafeGuard Enterprise Datenbank auf mehrere SQL Server replizieren. Für Informationen zum Aufsetzen der Datenbankreplizierung, *siehe Replikation der SafeGuard Enterprise Datenbank* (Seite 84)

Sie können mehrere SafeGuard Enterprise Datenbanken für unterschiedliche Mandanten, z. B. Firmenstandorte, Organisationseinheiten oder Domänen, einrichten und verwalten. Für Informationen zum Konfigurieren von Multi Tenancy, *siehe Multi Tenancy Konfigurationen* (Seite 35).

Hinweis:

Wir empfehlen den Einsatz eines permanenten Online-Backups für die Datenbank. Führen Sie ein regelmäßiges Backup Ihrer Datenbank durch, um Schlüssel, Unternehmenszertifikate und Benutzer-Computer-Zuordnungen zu sichern. Beispiele für empfohlene Backup-Zyklen: nach dem Erstimport der Daten, nach größeren Änderungen oder in turnusmäßigen Abständen, z. B. wöchentlich oder täglich.

5.1 Datenbank-Authentisierung

Um auf die SafeGuard Enterprise Datenbank zuzugreifen, muss sich der erste Sicherheitsbeauftragte des SafeGuard Management Centers am SQL Server authentisieren. Es gibt folgende Möglichkeiten:

- Windows-Authentisierung: ernennen Sie einen vorhandenen Windows-Benutzer zum SQL-Benutzer
- SQL-Authentisierung: richten Sie ein SQL-Benutzerkonto ein.

Fragen Sie Ihren SQL-Administrator, welche Form der Authentisierung für Sie als Sicherheitsbeauftragter vorgesehen ist. Sie benötigen diese Information vor der Erzeugung der Datenbank und vor der Erstkonfiguration des SafeGuard Management Centers im SafeGuard Management Center Konfigurationsassistenten.

Verwenden Sie SQL-Authentisierung für Computer, die sich nicht in einer Domäne befinden. Ansonsten verwenden Sie Windows-Authentisierung. Wenn Sie SQL-Authentisierung einsetzen, empfehlen wir, die Verbindung zu und vom Datenbankserver durch SSL zu sichern. Für weitere Informationen, *siehe Einrichten von SSL* (Seite 9).

5.1.1 Datenbankzugriffsrechte

SafeGuard Enterprise ist so eingerichtet, dass es für das Zusammenspiel mit der SQL-Datenbank nur ein einziges Benutzerkonto mit minimalen Zugriffsberechtigungen auf die Datenbank benötigt. Dieses Benutzerkonto wird vom SafeGuard Management Center genutzt und lediglich auf den ersten Sicherheitsbeauftragten des SafeGuard Management Centers ausgestellt. Damit ist die Verbindung zur SafeGuard Enterprise Datenbank gewährleistet. Während des Betriebs von SafeGuard Enterprise benötigt ein einziger Sicherheitsbeauftragter des SafeGuard Management Centers nur die Lese/Schreib-Berechtigung für die SafeGuard Enterprise Datenbank.

Die SafeGuard Enterprise Datenbank kann entweder manuell oder automatisch während der Erstkonfiguration im SafeGuard Management Center erzeugt werden. Soll die Datenbank automatisch erstellt werden, so sind für den ersten SafeGuard Management Center Sicherheitsbeauftragten erweiterte Zugriffsrechte für die SQL Datenbank (db_creator) erforderlich. Diese Berechtigungen können dem Sicherheitsbeauftragten danach vom SQL-Administrator aber wieder bis zur nächsten Installation/Aktualisierung entzogen werden.

Wenn die Erweiterung der Rechte während der Installation des SafeGuard Management Centers nicht gewünscht ist, kann der SQL-Administrator die SafeGuard Enterprise Datenbank per Skript erzeugen. Dazu können die beiden Skripts **CreateDatabase.sql** und **CreateTables.sql** aus der Produktlieferung ausgeführt werden.

Die folgende Tabelle zeigt die notwendigen SQL-Berechtigungen für die unterschiedlichen Versionen von Microsoft SQL Server.

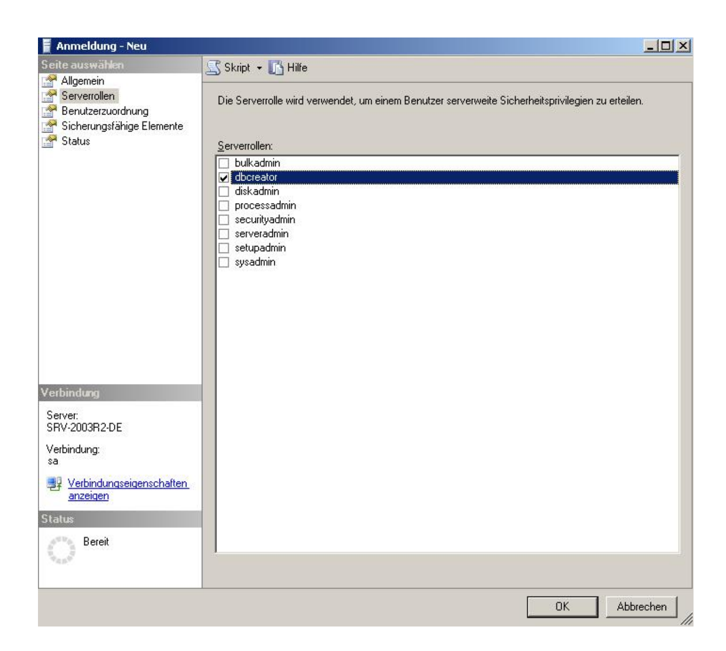
Zugriffsberechtigung	SQL Server 2005, SQL Server 2005 Express	SQL Server 2008, SQL Server 2008 Express
Datenbank erstellen		
Server	db_creator	db_creator
Master Datenbank	keine	keine
SafeGuard Enterprise Datenbank	db_ownerpublic (Standard)	db_ownerpublic (Standard)
Datenbank benutzen		
Server	keine	keine
Master Datenbank	keine	keine
SafeGuard Enterprise Datenbank	db_datareaderdd b_datawriter public (Standard)	db_datareader db_datawriter public (Standard)

5.1.2 Erstellen eines Windows-Benutzerkontos für die Anmeldung am SQL Server

Die folgende Beschreibung der einzelnen Konfigurationsschritte wendet sich an SQL-Administratoren und bezieht sich auf Microsoft Windows Server 2008 und Microsoft SQL Server 2005, Standard oder Express Edition. Für Informationen zur Windows-Authentisierung mit Windows Server 2003 und SQL Server 2005, siehe: *http://www.sophos.de/support/knowledgebase/article/108339.html*

Als SQL-Administrator benötigen Sie das Recht, Benutzerkonten zu erstellen.

1. Öffnen Sie SQL Server Management Studio. Melden Sie sich am SQL Server mit Ihren Anmeldeinformationen an.
2. Öffnen Sie den **Objekt-Explorer**, klicken Sie mit der rechten Maustaste auf **Sicherheit**, wählen Sie **Neu** und klicken Sie dann auf **Anmeldungen**.
3. Wählen Sie unter **Anmeldung - Neu** auf der **Allgemein** Seite die Option **Windows-Authentifizierung**.
4. Klicken Sie auf **Suchen**. Suchen Sie nach dem relevanten Windows-Benutzernamen und klicken Sie auf **OK**. Der Benutzername wird als **Anmeldename** angezeigt.
5. Wenn noch keine SafeGuard Enterprise Datenbank durch ein Skript angelegt wurde, wählen Sie unter **Standarddatenbank** die Option **Master**.
6. Klicken Sie auf **OK**.
7. Um die Datenbank automatisch während der Konfiguration des SafeGuard Management Center zu erstellen, müssen Sie die Zugriffsrechte wie folgt ändern: Weisen Sie jetzt unter **Anmeldung - Neu** unter **Allgemein** die Zugangsberechtigungen/Rollen zu, indem Sie links auf **Serverrollen** klicken. Wählen Sie **dbcreator**. Nach der Installation von SafeGuard Enterprise kann die Datenbankrolle auf **dbowner** zurückgesetzt werden.



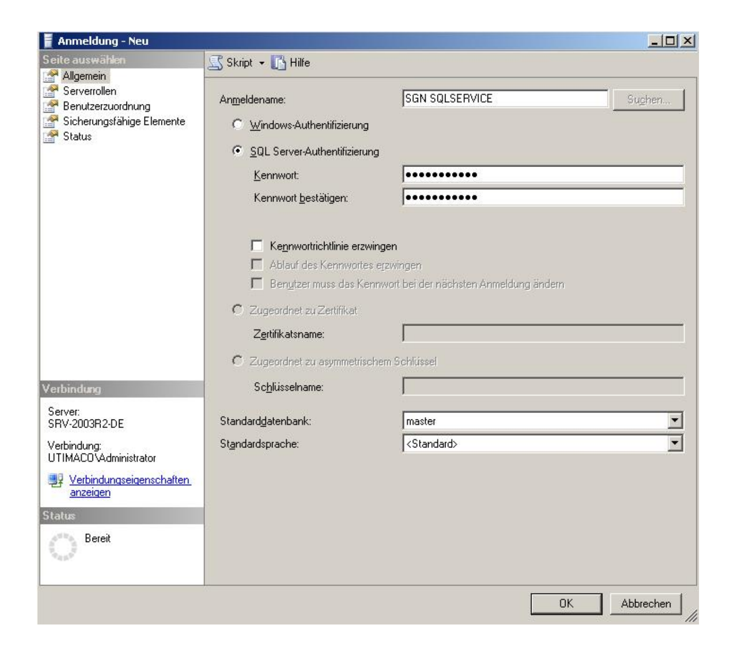
5.1.3 Erstellen eines SQL-Kontos für die Anmeldung am SQL Server

Die nachfolgende Beschreibung der einzelnen Konfigurationsschritte richtet sich an SQL-Administratoren. Sie bezieht sich auf Microsoft Windows Server 2003 mit Microsoft SQL Server 2005 und auf alle Editionen von Microsoft Windows Server 2008 mit der Standardedition von Microsoft SQL Server 2008.

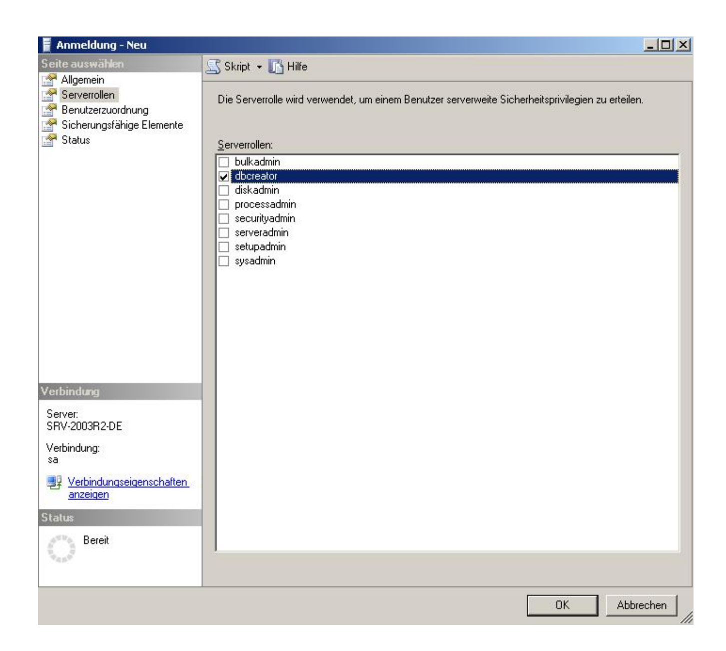
Als SQL-Administrator benötigen Sie das Recht, ein SQL-Benutzerkonto zu erstellen.

1. Öffnen Sie SQL Server Management Studio. Melden Sie sich am SQL Server mit Ihren Anmeldeinformationen an.
2. Öffnen Sie den **Objekt-Explorer**, klicken Sie mit der rechten Maustaste auf **Sicherheit**, wählen Sie **Neu** und klicken Sie dann auf **Anmeldungen**.
3. Wählen Sie unter **Anmeldung - Neu** auf der **Allgemein** Seite die Option **SQL Server Authentifizierung**.
4. Führen Sie auf der **Allgemein** Seite bei **Anmeldename** folgende Schritte durch:
   a) Geben Sie den Namen des neuen Benutzers ein, z. B. SGN SQLSERVICE.
   b) Geben Sie ein Kennwort für das Konto ein und bestätigen Sie es.
   c) Deaktivieren Sie **Kennwortrichtlinie erzwingen**.
   d) Wenn noch keine SafeGuard Enterprise Datenbank durch ein Skript angelegt wurde, wählen Sie unter **Standarddatenbank** die Option **Master**. Klicken Sie auf **OK**.

   Notieren Sie sich die Authentisierungsmethode und die Anmeldedaten. Sie müssen diese dem SafeGuard Management Center Sicherheitsbeauftragten mitteilen.



5. Um die Datenbank automatisch während der Konfiguration des SafeGuard Management Center zu erstellen, müssen Sie die Zugriffsrechte wie folgt ändern: Weisen Sie jetzt unter **Anmeldung - Neu** unter **Allgemein** die Zugangsberechtigungen/Rollen zu, indem Sie links auf **Serverrollen** klicken. Wählen Sie **dbcreator**. Nach der Installation von SafeGuard Enterprise kann die Datenbankrolle auf **dbowner** zurückgesetzt werden.



Das SQL-Benutzerkonto und die Zugriffsberechtigungen sind damit für den SafeGuard Enterprise Sicherheitsbeauftragten eingerichtet.

5.2 Erzeugen der SafeGuard Enterprise Datenbank

Nachdem das Benutzerkonto für die SQL Server Anmeldung eingerichtet ist, können Sie die SafeGuard Enterprise Datenbank erzeugen. Hier gibt es zwei Möglichkeiten:

- im Konfigurationsassistenten für das SafeGuard Management Center

  Als Sicherheitsbeauftragter können Sie die SafeGuard Enterprise Datenbank während der Erstkonfiguration im SafeGuard Management Centers leicht und bequem erstellen. Der SafeGuard Management Center Konfigurationsassistent führt Sie durch die Basiskonfiguration, zu der auch die Erstellung der Datenbank gehört. Installieren und konfigurieren Sie hierzu zuerst das SafeGuard Management Center, *siehe Einrichten des SafeGuard Management Centers* (Seite 33) und ändern Sie dann die Zugriffsrechte für die SafeGuard Enterprise Datenbank *siehe Ändern der Zugriffsrechte für die SafeGuard Enterprise Datenbank* (Seite 29).

- Mit SQL Skripts, die in der Produktlieferung zur Verfügung stehen.

  Dieser Weg ist dann angebracht, wenn die Erweiterung der Datenbankberechtigung während der Installation des SafeGuard Management Centers nicht gewünscht ist.

  Es hängt von Ihrer Unternehmensumgebung ab, welche Methode Sie anwenden. Am besten sollte dies zwischen SQL-Administrator und SafeGuard Enterprise Sicherheitsbeauftragten vorab geklärt werden.

5.2.1 Erzeugen der SafeGuard Enterprise Datenbank per Skript

Wenn Sie die SafeGuard Datenbank automatisch während der Konfiguration des SafeGuard Management Center erzeugen möchten, können Sie diesen Schritt überspringen. Wenn erweiterte SQL-Berechtigungen während der SafeGuard Management Center Konfiguration nicht erwünscht sind, führen Sie diesen Schritt aus. Dazu stehen im Tools-Verzeichnis der Produktlieferung zwei Skripts zur Verfügung:

- CreateDatabase.sql
- CreateTables.sql

Die folgende Beschreibung der Arbeitsschritte wendet sich an SQL-Administratoren und bezieht sich auf Microsoft SQL Server 2008 Standard Edition.

Als SQL-Administrator benötigen Sie das Recht zum Erstellen einer Datenbank.

1. Kopieren Sie die Skripts CreateDatabase.sql und CreateTables.sql aus der SafeGuard Enterprise Produktlieferung auf den SQL Server.
2. Starten Sie das Skript **CreateDatabase.sql** durch Doppelklick. Das Programm SQL Server Management Studio wird aufgerufen.
3. Melden Sie sich am SQL Server mit Ihren Anmeldeinformationen an.
4. Überprüfen Sie, ob die beiden Zielpfade, die zu Beginn des Skripts unter **FILENAME** (MDF, LDF) angegeben sind, auf der lokalen Festplatte vorhanden sind. Korrigieren Sie sie, wenn nötig.
5. Klicken Sie auf die Schaltfläche **Ausführen**, um die Datenbank zu erzeugen. Sie haben die Datenbank **SafeGuard** angelegt. Erzeugen Sie anschließend die Tabellen mit Hilfe des Skripts CreateTables.sql aus der Produktlieferung.
6. Doppelklicken Sie auf **CreateTables.sql**. Ein weiterer Bereich wird in Microsoft SQL Server Management Studio geöffnet.
7. Geben Sie am Beginn des Skripts **use SafeGuard** ein, um die SafeGuard Enterprise Datenbank auszuwählen, in der die Tabellen erstellt werden sollen.
8. Klicken Sie auf die Schaltfläche **Ausführen**, um die Datenbank zu erzeugen.

Die SafeGuard Enterprise Datenbank und die zugehörigen Tabellen werden erstellt.

5.3 Ändern der Zugriffsrechte für die SafeGuard Enterprise Datenbank

Nach dem Erstellen der SafeGuard Enterprise Datenbank, entweder per Skript oder im SafeGuard Management Center, können die Zugriffsrechte wieder geändert werden. Da es möglich ist, einem Benutzer für eine Datenbank unterschiedliche Rollen und Berechtigungen zuzuweisen, werden nur die Rechte beschrieben, die für die Herstellung einer Verbindung zur SafeGuard Enterprise Datenbank mindestens erforderlich sind.

1. Öffnen Sie SQL Server Management Studio. Melden Sie sich am SQL Server mit Ihren Anmeldeinformationen an.
2. Öffnen Sie den **Objekt-Explorer**, klicken Sie mit der rechten Maustaste auf **Sicherheit** und dann auf **Anmeldungen**.

3. Klicken Sie mit der rechten Maustaste auf den erforderlichen Benutzer und wählen Sie **Eigenschaften**.
4. Wählen Sie **Benutzerzuordnung** auf der linken Seite. Wählen Sie unter **Users mapped to this login** (**Benutzer, die dieser Anmeldung zugeordnet sind**) die Datenbank **SafeGuard**.
5. Stellen Sie unter **Database role membership for** (**Datenbankrollenmitgliedschaft für**) die Zugriffsrechte für die Benutzung der SafeGuard Enterprise Datenbank ein: wählen Sie **db_datareader**, **db_datawriter** und **public**.
6. Klicken Sie auf **OK**.

5.4 Überprüfung von Einstellungen für SQL-Dienste, Named Pipes und TCP/IP

Diese Beschreibung bezieht sich auf Microsoft Windows Server 2008 (R2) und Microsoft SQL Server 2008 Standard oder Express Edition.

1. Öffnen Sie den SQL Server-Konfigurations-Manager.
2. Wählen Sie in der Navigationsstruktur auf der linken Seite **SQL Server-Dienste**.
3. Überprüfen Sie, ob der **Status** von **SQL Server** und **SQL Server Browser Läuft** und der **Startmodus Automatisch** ist.
4. Wählen Sie in der Navigationsstruktur auf der linken Seite **SQL Server-Netzwerkkonfiguration**.
5. Klicken Sie mit der rechten Maustaste auf das Protokoll **Named Pipes** und wählen Sie **Aktiviert**.
6. Klicken Sie mit der rechten Maustaste auf das Protokoll **TCP/IP** und wählen Sie **Aktiviert**.
7. Klicken Sie außerdem mit der rechten Maustaste auf das Protokoll **TCP/IP** und wählen Sie **Eigenschaften**. Belassen Sie in der Registerkarte **IP-Adressen** unter **IPAlll** das Feld **Dynamische TCP-Ports** leer. Geben Sie im Feld **TCP Port** 1433 ein.
8. Starten Sie die SQL-Dienste neu.

5.5 Erstellen einer Windows Firewall Regel auf Windows Server 2008 (R2)

Diese Beschreibung bezieht sich auf Microsoft Windows Server 2008 (R2) mit Microsoft SQL Server 2008 Standard oder Express Edition. Wenn Sie diese Konfiguration verwenden, führen Sie die nachfolgend angegebenen Schritte aus um sicherzustellen, dass eine Verbindung zwischen der SafeGuard Enterprise Datenbank und dem SafeGuard Management Center hergestellt werden kann.

1. Klicken Sie auf dem Computer, der als Host für die SQL Server Instanz dient, auf **Start** und dann auf **Verwaltung**. Wählen Sie **Windows-Firewall mit erweiterter Sicherheit**.
2. Wählen Sie in der Navigationsstruktur auf der linken Seite **Eingehende Regeln**.
3. Klicken Sie in der Menüleiste auf **Aktion** und wählen Sie **Neue Regel**. Der Assistent für neue eingehende Regeln wird gestartet.
4. Wählen Sie auf der **Regeltyp** Seite **Benutzerdefiniert** und klicken Sie auf **Weiter**.

5. Wählen Sie auf der **Programm** Seite die Programme und Dienste, auf die diese Regel angewendet werden soll. Klicken Sie dann auf **Weiter**.
6. Wählen Sie auf der **Protokolle und Ports** Seite **TCP** als **Protokolltyp**. Wählen Sie für **Lokaler Port** die Option **Bestimmte Ports** und geben Sie **1433** ein. Wählen Sie für **Remoteport** die Option **Alle Ports**. Klicken Sie auf **Weiter**.
7. Auf der **Bereich** Seite können Sie festlegen, dass die Regel nur für den Netzverkehr von oder an die auf dieser Seite angegebenen IP-Adressen gilt. Nehmen Sie die entsprechende Konfiguration vor und klicken Sie auf **Weiter**.
8. Wählen Sie auf der **Aktion** Seite die Option **Verbindung zulassen** und klicken Sie auf **Weiter**.
9. Geben Sie auf der **Profil** Seite an, wo die Regel angewendet werden soll. Klicken Sie dann auf **Weiter**.
10. Geben Sie auf der **Name** Seite einen Namen und eine Beschreibung für Ihre Regel ein und klicken Sie auf **Beenden**.

5.6 Durchführen von weiteren Konfigurationsschritten bei Benutzung eines Windows-Benutzerkontos für die Anmeldung am SQL Server

Diese Beschreibung bezieht sich auf Microsoft Windows Server 2008 (R2) mit Microsoft SQL Server 2008 Standard oder Express Edition. Für Informationen zur Windows-Authentisierung mit Windows Server 2003 und SQL Server 2005, siehe:
http://www.sophos.de/support/knowledgebase/article/108339.html

Um die Kommunikation zwischen dem SafeGuard Enterprise Server und der SafeGuard Enterprise Datenbank bei Anwendung der Windows-Authentisierung zu ermöglichen, muss der Benutzer zu einem Mitglied von Active Directory Gruppen gemacht werden. Die Berechtigungen für lokale Dateien müssen angepasst werden und das SQL Benutzerkonto muss in den Anwendungspool des IIS aufgenommen werden.

1. Wählen Sie **Start** und dann **Ausführen**. Geben Sie **dsa.msc** ein. Öffnen Sie das Active Directory Users and Computers Snap-in.
2. Klappen Sie in der Navigationsstruktur auf der linken Seite die Domänenstruktur aus und wählen Sie **Builtin**.
3. Fügen Sie den relevanten Windows-Benutzer zu folgenden Gruppen hinzu: IIS_IUSRS, Performance Log Users, Performance Monitor Users.
4. Beenden Sie das Snap-in.
5. Klicken Sie im lokalen Dateisystem im Windows Explorer mit der rechten Taste auf den C:\Windows\Temp Ordner und wählen Sie **Sicherheit**.
6. Klicken Sie in **Sicherheit** auf **Hinzufügen** und geben Sie unter **Objektname** den entsprechenden Windows-Benutzernamen ein. Klicken Sie auf **OK**.
7. Wählen Sie in **Sicherheit** unter **Berechtigungen Spezielle Berechtigungen** und setzen Sie im **Objekt** Dialog die folgenden Berechtigungen auf **Zulassen**: **Dateien erstellen / Daten schreiben**, **Löschen** und **Lesen**.
8. Klicken Sie auf **OK** und beenden Sie den Windows Explorer.
9. Öffnen Sie den **Internet Information Services Manager**.

10. Wählen Sie im **Verbindungen** Bereich auf der linken Seite die **Anwendungspools** für den relevanten Server-Knoten.
11. Wählen Sie aus der **Anwendungspools** Liste auf der rechten Seite **SGNSRV-Pool**.
12. Wählen Sie im **Aktionen** Bereich auf der linken Seite **Erweiterte Einstellungen**.
13. Klicken Sie in **Erweiterte Einstellungen** unter **Prozessmodell** für die Eigenschaft **Identität** auf die **...** Schaltfläche.
14. Wählen Sie in **Identität des Anwendungspools** die Option **Benutzerdefiniertes Konto** und klicken Sie auf **Festlegen**.
15. Geben Sie in **Anmeldeinformationen festlegen** den relevanten Windows-Benutzernamen in folgender Form ein: **Domäne\Windows-Benutzername**. Geben Sie das entsprechende Windows-Kennwort ein, bestätigen Sie es und klicken Sie auf **OK**.
16. Wählen Sie im Bereich **Verbindungen** auf der linken Seite den relevanten Server-Knoten und klicken Sie im **Aktionen** Bereich auf **Neu starten**.
17. Wählen Sie im Bereich **Verbindungen** auf der linken Seite unter dem relevanten Server-Knoten unter **Sites Standard-Websites** die Option **SGNSRV**.
18. Wählen Sie im **Aktionen** Bereich auf der rechten Seite die Option **Authentifizierung**.
19. Klicken Sie mit der rechten Maustaste auf **Anonyme Authentifizierung** und wählen Sie **Bearbeiten**.
20. Wählen Sie bei **Identität des anonymen Benutzers** die Option **Bestimmter Benutzer** und überprüfen Sie, ob der Benutzername **IUSR** lautet. Korrigieren Sie ihn, wenn nötig.
21. Klicken Sie auf **OK**.

Die zusätzliche Konfiguration für die Benutzung eines Windows-Kontos für die Anmeldung am SQL Server ist nun abgeschlossen.

6 Einrichten des SafeGuard Management Centers

Dieses Kapitel beschreibt die Installation und Konfiguration des SafeGuard Management Centers.

Das SafeGuard Management Center ist das zentrale Verwaltungswerkzeug für SafeGuard Enterprise. Installieren Sie es auf den Administrator-Computern, die Sie für die Verwaltung von SafeGuard Enterprise einsetzen möchten. Das SafeGuard Management Center muss nicht notwendigerweise nur auf einem Computer installiert sein. Es kann auf jedem Rechner im Netzwerk installiert sein, von wo aus auf die SafeGuard Enterprise Datenbanken zugegriffen werden kann.

Mit datenbankspezifischen Konfigurationen (Multi Tenancy) ermöglicht das SafeGuard Management Center den Einsatz von SafeGuard Enterprise mit mehreren Datenbanken. Sie können verschiedene SafeGuard Enterprise Datenbanken für unterschiedliche Bereiche (z. B. Unternehmensstandorte, Organisationseinheiten oder Domänen) einrichten und verwalten. Um den Verwaltungsaufwand zu reduzieren, können Sie Datenbankkonfigurationen auch in Dateien exportieren und aus Dateien importieren.

6.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.
- .NET Framework 3.0 Service Pack 1 ist installiert.

  .NET Framework ist kostenlos verfügbar. Sie finden das Programm z. B. auf Ihrer Windows-DVD. Je nach Windows-Version wird es bereits als Standard mit installiert. Sie können das Programm auch herunterladen: *http://microsoft.com/downloads*.
- Wenn Sie eine neue SafeGuard Enterprise Datenbank während der SafeGuard Management Center Konfiguration erzeugen wollen, benötigen Sie entsprechende SQL-Zugriffsberechtigungen, *siehe Datenbankzugriffsrechte* (Seite 25).

6.2 Installieren des SafeGuard Management Center

1. Starten Sie SGNManangementCenter.msi aus dem Installationsordner Ihrer Produktlieferung. Ein Assistent führt Sie durch die notwendigen Schritte.
2. Klicken Sie auf der Willkommenseite auf **Weiter**.
3. Akzeptieren Sie die Lizenzvereinbarung.
4. Übernehmen Sie den Standardinstallationspfad.
5. Wählen Sie den Installationstyp aus:

   - Wenn das SafeGuard Management Center nur eine Datenbank unterstützen soll, wählen Sie eine Installation vom Typ **Typisch** aus.
   - Wenn das SafeGuard Management Center mehrere Datenbanken unterstützen soll (**Multi Tenancy**), wählen Sie eine Installation vom Typ **Typisch** aus. Für weitere Informationen, *siehe Multi Tenancy Konfigurationen* (Seite 35).

6. Klicken Sie auf **Beenden**, um die Installation abzuschließen.

Das SafeGuard Management Center ist installiert. Starten Sie Ihren ggf. Computer neu. Im nächsten Schritt führen Sie die Erstkonfiguration im SafeGuard Management Center durch.

6.3 Anzeigen des SafeGuard Management Center Hilfesystems

Das SafeGuard Management Center Hilfesystem wird in Ihrem Browser angezeigt. Es bietet umfassende Features wie kontextsensitive Hilfe und Volltextsuche. Das Hilfesystem ist für die volle Funktionalität der Inhaltsseiten konfiguriert und aktiviert JavaScript in Ihrem Browser.

Beim Microsoft Internet Explorer zeigt sich folgendes Verhalten:

- Windows XP/Windows Vista/Windows 7 - Internet Explorer 6/7/8 - Standardsicherheit:

  Es wird keine Sicherheitsleiste angezeigt, die angibt, dass der Internet Explorer die Scripting-Ausführung gesperrt hat.
  JavaScript wird ausgeführt.

- Windows 2003 Server Enterprise Edition - Internet Explorer 6 - Erweiterte Sicherheitskonfiguration (Standardinstallationskonfiguration):

  Eine Informationsbox gibt an, dass die erweiterte Sicherheitskonfiguration aktiviert ist und die Seite das Scripting ausführt. Sie können diese Meldung deaktivieren.
  JavaScript wird ausgeführt.

Hinweis:

Auch wenn JavaScript deaktiviert ist, können Sie das SafeGuard Management Center Hilfesystem aufrufen und im System navigieren. Bestimmte Funktionen, z. B. die Suche, lassen sich dann jedoch nicht anzeigen.

6.4 Konfigurieren des SafeGuard Management Centers

Nach der Installation müssen Sie das SafeGuard Management Center konfigurieren. Der SafeGuard Management Center Konfigurationsassistent unterstützt Sie bei der Erstkonfiguration durch Hilfestellung bei der Definition der grundlegenden SafeGuard Management Center Einstellungen sowie bei der Konfiguration der Datenbankverbindung. Der Assistent wird automatisch aufgerufen, wenn Sie das SafeGuard Management Center zum ersten Mal nach der Installation starten.

Sie können das SafeGuard Management Center für die Anwendung mit einer oder mehreren Datenbank (Multi Tenancy) konfigurieren.

Hinweis:

Die folgenden Schritte müssen mit dem Konfigurationsassistenten sowohl für Single Tenancy als auch für Multi Tenancy Konfigurationen ausgeführt werden.

6.4.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.
- Halten Sie die folgenden Informationen bereit. Diese erhalten Sie ggf. von Ihrem SQL-Administrator.

  SQL Anmeldeinformationen
  Name des SQL Servers, auf dem die SafeGuard Enterprise Datenbank laufen soll.
  Name der SafeGuard Enterprise Datenbank, falls diese bereits erzeugt wurde.

6.4.2 Multi Tenancy Konfigurationen

Sie können mehrere verschiedene SafeGuard Enterprise Datenbankkonfigurationen für eine Instanz des SafeGuard Management Centers konfigurieren und verwalten. Dies erweist sich vor allem dann als nützlich, wenn Sie verschiedene Konfigurationen für verschiedene Domänen, Organisationseinheiten oder Unternehmensstandorte einsetzen möchten.

Hinweis:

Sie müssen pro Datenbank (Mandant) jeweils eine separate SafeGuard Enterprise Server Instanz einrichten.

Zur Vereinfachung der Konfiguration können neu erstellte Datenbankkonfigurationen zur späteren Wiederverwendung in eine Datei exportiert werden und zuvor erstellte Konfigurationen aus einer Datei eingelesen werden.

Um das SafeGuard Management Center für Multi Tenancy zu konfigurieren, führen Sie zunächst die initiale Konfiguration und danach weitere spezifische Schritte für die Multi Tenancy Konfiguration durch.

6.4.3 Starten der Erstkonfiguration des SafeGuard Management Center

Nach der Installation des SafeGuard Management Center, müssen Sie die Erstkonfiguration durchführen. Die Erstkonfiguration muss sowohl für den Single Tenancy als auch für den Multi Tenancy Modus ausgeführt werden.

So starten Sie den SafeGuard Management Center Konfigurationsassistenten:

1. Starten Sie das **SafeGuard Management Center** über das **Start** Menü. Der Konfigurationsassistent wird gestartet und führt Sie durch die notwendigen Schritte.
2. Klicken Sie auf der **Willkommen** Seite auf **Weiter**.

6.4.4 Konfigurieren der Datenbankserver-Verbindung

Zum Speichern aller SafeGuard Enterprise spezifischen Verschlüsselungsrichtlinien und Einstellungen wird eine Datenbank verwendet. Damit das SafeGuard Management Center mit dem SafeGuard Enterprise Server kommunizieren kann, müssen Sie eine

Authentisierungsmethode für den Zugriff auf die Datenbank festlegen, entweder Windows NT Authentisierung oder SQL-Authentisierung. Wenn Sie eine Verbindung zum Datenbankserver mit SQL Authentisierung herstellen möchten, stellen Sie sicher, dass Sie die notwendigen SQL-Anmeldedaten zur Hand haben. Falls notwendig, erhalten Sie diese Informationen von Ihrem SQL Administrator.

1. Führen Sie auf der Seite **Datenbankserver-Verbindung** folgende Schritte aus:
   - Wählen Sie unter **Verbindungseinstellungen** den SQL-Datenbankserver aus der **Datenbankserver** Liste aus. Es werden alle Rechner eines Netzwerks aufgelistet, auf denen ein Microsoft SQL Server installiert ist. Wenn der Server nicht auswählbar ist, tragen Sie Servername bzw. IP-Adresse mit dem SQL-Instanznamen manuell ein.
   - Aktivieren Sie **SSL verwenden**, um die Verbindung zwischen SafeGuard Management Center und SQL-Datenbankserver zu sichern. Wenn Sie **SQL Server Authentisierung** ausgewählt haben, empfehlen wir dringend, diese Einstellung zu aktivieren, da dadurch der Transport der SQL-Anmeldedaten verschlüsselt wird. SSL-Verschlüsselung erfordert eine funktionsfähige SSL- Umgebung auf dem SQL Datenbankserver, die Sie vorab einrichten müssen, *siehe Sichern von Transportverbindungen mit SSL* (Seite 9).

2. Wählen Sie unter **Authentisierung** die Art der Authentisierung, die für den Zugriff auf die Datenbankserverinstanz benutzt werden soll. Dies ist erforderlich, damit das SafeGuard Management Center mit der Datenbank kommunizieren kann:
   - Aktivieren Sie **Windows NT Authentisierung verwenden**, um Ihre Windows-Anmeldedaten zu verwenden.

     Hinweis:

     Verwenden Sie diese Art der Authentisierung, wenn Ihr Computer Teil einer Domäne ist. Es sind jedoch noch zusätzliche Konfigurationsschritte erforderlich, da der Benutzer zur Herstellung einer Verbindung mit der Datenbank berechtigt sein muss, *siehe Erstellen eines Windows-Benutzerkontos für die Anmeldung am SQL Server* (Seite 26) und *siehe Durchführen von weiteren Konfigurationsschritten bei Benutzung eines Windows-Benutzerkontos für die Anmeldung am SQL Server* (Seite 31).

   - Aktivieren Sie **SQL Server Authentisierung verwenden**, um mit den entsprechenden SQL-Anmeldeinformationen auf die Datenbank zuzugreifen. Geben Sie die Anmeldeinformationen des SQL-Benutzerkontos ein, das Ihr SQL-Administrator erstellt hat. Falls notwendig, erhalten Sie diese Informationen von Ihrem SQL Administrator.

     Hinweis:

     Verwenden Sie diese Art der Authentisierung, wenn Ihr Computer keiner Domäne angehört. Aktivieren Sie **SSL verwenden**, um die Verbindung zum und vom Datenbankserver zu sichern.

3. Klicken Sie auf **Weiter**.

Die Verbindung zum Datenbankserver ist hergestellt.

6.4.5 Erstellen oder Auswählen einer Datenbank

Legen Sie auf der Seite **Datenbankeinstellungen** fest, ob eine existierende Datenbank oder eine neue Datenbank zum Speichern der Administrationsdaten benutzt werden soll.

1. Gehen Sie wie folgt vor:
   - Wenn noch keine Datenbank existiert, wählen Sie **Eine neue Datenbank mit folgendem Namen erstellen**. Geben Sie einen Namen für die neue Datenbank ein. Sie benötigen dazu die entsprechenden SQL-Zugriffsberechtigungen, *siehe Datenbankzugriffsrechte* (Seite 25). Um Probleme zu vermeiden, sollten in SafeGuard Enterprise Datenbanknamen nur folgende Zeichen verwendet werden: Buchstaben (A - Z, a - z), Zahlen (0 - 9), Unterstriche (_).
   - Wenn bereits eine Datenbank angelegt wurde oder wenn Sie das SafeGuard Management Center bereits auf einem anderen Computer installiert haben, klicken Sie auf **Folgende bestehende Datenbank wählen** und wählen Sie die entsprechende Datenbank aus der Liste aus.
2. Klicken Sie auf **Weiter**.

6.4.6 Erstellen eines Haupt-Sicherheitsbeauftragten (Master Security Officer, MSO)

Als Sicherheitsbeauftragter melden Sie sich am SafeGuard Management Center an, um SafeGuard Enterprise Richtlinien zu erstellen und die Verschlüsselungssoftware für die Endbenutzer zu konfigurieren.

Der Haupt-Sicherheitsbeauftragte (MSO) ist der Administrator höchster Ebene mit allen Rechten und einem Zertifikat, das nicht abläuft.

1. Geben Sie auf der Seite **Daten des Sicherheitsbeauftragten** unter **Haupt-Sicherheitsbeauftragten-ID** einen Namen für den Haupt-Sicherheitsbeauftragten ein.
2. Geben Sie unter **Anmeldung mit Token** an, ob Sie einen Token/eine Smartcard für die Anmeldung benutzen möchten oder nicht.

   Wir empfehlen, dass Sie die Anmeldung mit Token nicht als **Zwingend erforderlich** definieren. Eine Anmeldung mit Token bzw. Smartcard erfordert eine gesonderte Konfiguration, die innerhalb des SafeGuard Management Centers zu erledigen ist.
3. Führen Sie auf der Seite **Zertifikat für den Haupt-Sicherheitsbeauftragten** einen der folgenden Schritte aus:
   - Klicken Sie auf **Erzeugen**, um ein neues Zertifikat für den Haupt-Sicherheitsbeauftragten zu erzeugen. Sie werden dazu aufgefordert, sowohl für den Zertifikatsspeicher als auch für die Datei, in die das Zertifikat exportiert werden soll (private Schlüsseldatei P12), jeweils ein Kennwort einzugeben und zu bestätigen. Das Zertifikat wird erzeugt und unter **Zertifikat für den Haupt-Sicherheitsbeauftragten** angezeigt.

- Klicken Sie auf **Importieren**, um ein Zertifikat für den Haupt-Sicherheitsbeauftragten zu verwenden, das bereits auf dem Netz zur Verfügung steht. Suchen Sie unter **Importieren des Zertifikats** die gesicherte Schlüsseldatei. Geben Sie unter **Kennwort der Datei** das für diese Datei festgelegte Kennwort ein und bestätigen Sie es. Wählen Sie **Schlüsseldatei im Zertifikatsspeicher speichern** und geben Sie das Kennwort für den Speicher ein. Klicken Sie auf **OK**. Das Zertifikat wird importiert und unter **Zertifikat für den Haupt-Sicherheitsbeauftragten** angezeigt.

Der Haupt-Sicherheitsbeauftragte benötigt das Kennwort des Zertifikatsspeichers für die Anmeldung am SafeGuard Management Center. Notieren Sie sich das Kennwort und bewahren Sie es an einem sicheren Ort auf. Steht das Kennwort nicht mehr zur Verfügung, so kann sich der Haupt-Sicherheitsbeauftragte nicht mehr am SafeGuard Management Center anmelden.

Für die Wiederherstellung einer beschädigten SafeGuard Management Center Installation benötigt der Haupt-Sicherheitsbeauftragte die private Schlüsseldatei.

4. Klicken Sie auf **Weiter**.

Der Haupt-Sicherheitsbeauftragte ist angelegt.

6.4.6.1 Erzeugen des Zertifikats des Haupt-Sicherheitsbeauftragten

Gehen Sie in **Zertifikat des Haupt-Sicherheitsbeauftragten erzeugen** folgendermaßen vor:

1. Bestätigen Sie unter **Haupt-Sicherheitsbeauftragten-ID** den Namen des Haupt-Sicherheitsbeauftragten.
2. Geben Sie nun zweimal das Kennwort für den Zertifikatsspeicher ein und klicken Sie auf **OK**.

Das Zertifikat des Haupt-Sicherheitsbeauftragten wird erzeugt und lokal als Backup (<mso_name>.cer) gespeichert.

Hinweis:

Notieren Sie sich das Kennwort und bewahren Sie es an einem sicheren Ort auf. Sie müssen sich am SafeGuard Management Center anmelden.

6.4.6.2 Export des Zertifikats des Haupt-Sicherheitsbeauftragten

Das Zertifikat des Haupt-Sicherheitsbeauftragten wird in eine Datei exportiert, die so genannte private Schlüsseldatei (P12). Diese ist mit einem Kennwort gesichert. Das Zertifikat des Haupt-Sicherheitsbeauftragten ist dadurch zusätzlich geschützt. Die private Schlüsseldatei wird für die Wiederherstellung einer beschädigten SafeGuard Management Center Installation benötigt.

So exportieren Sie das Zertifikat eines Haupt-Sicherheitsbeauftragten:

1. Geben Sie unter **Zertifikat exportieren** ein Kennwort für den privaten Schlüssel (P12-Datei) ein und bestätigen Sie es. Das Kennwort muss aus 8 alphanumerischen Zeichen bestehen.
2. Klicken Sie auf **OK**.
3. Geben Sie einen Speicherort für die private Schlüsseldatei ein.

Die private Schlüsseldatei wird erzeugt und die Datei wird am angegebenen Speicherort gespeichert <mso_name.p12).

Hinweis:

Erstellen Sie eine Sicherungskopie des privaten Schlüssels (P12-Datei) und legen Sie diese direkt nach der Erstkonfiguration an einem sicheren Speicherort ab. Andernfalls führt ein eventueller PC-Absturz zum Verlust des Schlüssels und SafeGuard Enterprise muss neu installiert werden. Das gilt für alle von SafeGuard Enterprise generierten Sicherheitsbeauftragten-Zertifikate. Weitere Informationen finden Sie in der Administrator-Hilfe im Kapitel *Unternehmenszertifikat und Master Security Officer Zertifikat exportieren*.

6.4.6.3 Import des Zertifikats des Haupt-Sicherheitsbeauftragten

Wenn bereits ein Zertifikat eines Haupt-Sicherheitsbeauftragten zur Verfügung steht, müssen Sie es in den Zertifikatsspeicher importieren.

Hinweis:

Ein Zertifikat kann nicht aus einer Microsoft PKI importiert werden. Ein importiertes Zertifikat muss minimal 1024 Bits haben und kann maximal 4096 Bits lang sein.

1. Klicken Sie unter **Authentisierungs-Schlüsseldatei importieren** auf die **[...]** Schaltfläche und wählen Sie die Schlüsseldatei aus. Geben Sie das **Kennwort der Schlüsseldatei** ein. Geben Sie das zuvor unter **Kennwort des Zertifikatsspeichers oder Token-PIN** definierte Kennwort für den Zertifikatsspeicher ein. Wählen Sie **In den Zertifikatsspeicher importieren** oder **Auf den Token kopieren**, um das Zertifikat auf einem Token zu speichern.
2. Geben Sie zur Initialisierung des Zertifikatsspeichers das Kennwort noch einmal ein.

Zertifikat und privater Schlüssel befinden sich nun im Zertifikatsspeicher. Zur Anmeldung an das SafeGuard Management Center wird das Kennwort des Zertifikatsspeichers verwendet.

6.4.7 Erzeugen des Unternehmenszertifikats

Mit dem Unternehmenszertifikat lassen sich unterschiedliche SafeGuard Management Center Installationen auseinander halten. In Verbindung mit dem Zertifikat des Haupt-Sicherheitsbeauftragten lässt sich mit dem Unternehmenszertifikat eine beschädigte SafeGuard Enterprise Datenbankkonfiguration wiederherstellen.

1. Wählen Sie auf der Seite **Unternehmenszertifikat** die Option **Neues Unternehmenszertifikat erzeugen**.
2. Geben Sie einen Namen Ihrer Wahl ein.
3. Klicken Sie auf **Weiter**.

Das neu angelegte Unternehmenszertifikat wird in der Datenbank gespeichert.

Erstellen Sie eine Sicherungskopie des Unternehmenszertifikats und legen Sie diese direkt nach der Erstkonfiguration an einem sicheren Speicherort ab.

Für Informationen zur Wiederherstellung einer korrupten Datenbankkonfiguration, *siehe Wiederherstellen einer beschädigten Datenbankkonfiguration* (Seite 44).

6.4.8 Abschließen der Erstkonfiguration des SafeGuard Management Center

1. Klicken Sie auf **Beenden**, um die Erstkonfiguration des SafeGuard Management Center abzuschließen.

Eine Konfigurationsdatei wird erstellt.

Ergebnis:

- Eine Verbindung zum SafeGuard Enterprise Server.
- Eine SafeGuard Enterprise Datenbank.
- Ein Haupt-Sicherheitsbeauftragten-Konto für die Anmeldung an das SafeGuard Management Center
- Alle notwendigen Zertifikate für die Wiederherstellung einer beschädigten Datenbankkonfiguration oder SafeGuard Management Center Installation

Sobald der Konfigurationsassistent geschlossen ist, wird das SafeGuard Management Center gestartet.

6.5 Erstellen weiterer Datenbankkonfigurationen (Multi Tenancy)

Voraussetzung: Die Funktion Multi Tenancy muss über eine Installation vom Typ **Vollständig** installiert worden sein. Die Erstkonfiguration des SafeGuard Management Center muss durchgeführt worden sein, *siehe Starten der Erstkonfiguration des SafeGuard Management Center* (Seite 35).

Hinweis:

Sie müssen pro Datenbank jeweils eine separate SafeGuard Enterprise Server Instanz einrichten.

So erstellen Sie eine weitere SafeGuard Enterprise Datenbankkonfiguration nach der Erstkonfiguration:

1. Starten Sie das SafeGuard Management Center. Der Dialog **Konfiguration auswählen** wird angezeigt.
2. Klicken Sie auf **Neu**. Der SafeGuard Management Center Konfigurationsassistent wird automatisch gestartet.
3. Der Assistent führt Sie durch die notwendigen Schritte für das Anlegen einer neuen Datenbankkonfiguration. Nehmen Sie die erforderlichen Einstellungen vor. Die neue Datenbankkonfiguration wird generiert.
4. Zur Authentisierung werden Sie dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird geöffnet und mit der ausgewählten Datenbankkonfiguration verbunden. Wenn Sie das SafeGuard Management Center das nächste Mal starten, können Sie die neue Datenbank-Konfiguration aus der Liste auswählen.

Hinweis:

Weitere Informationen zu Multi Tenancy finden Sie in der Administratorhilfe im Kapitel *Mit mehreren Datenbankkonfigurationen arbeiten*.

6.6 Konfigurieren zusätzlicher Instanzen des SafeGuard Management Center

Sie können zusätzliche Instanzen des SafeGuard Management Center konfigurieren, um Sicherheitsbeauftragten den Zugriff für die Durchführung administrativer Aufgaben auf verschiedenen Computern zu ermöglichen. Das SafeGuard Management Center kann auf jedem Rechner im Netzwerk installiert sein, von wo aus auf die Datenbank zugegriffen werden kann.

SafeGuard Enterprise verwaltet die Zugriffsrechte auf das SafeGuard Management Center in einem eigenen Zertifikatsverzeichnis. In diesem Verzeichnis müssen die Zertifikate aller Sicherheitsbeauftragten, die sich am SafeGuard Management Center anmelden dürfen, vorhanden sein. Für die Anmeldung an das SafeGuard Management Center ist dann nur das Kennwort für den Zertifikatsspeicher erforderlich.

1. Installieren Sie SGNManagementCenter.msi mit den gewünschten Features auf einem weiteren Computer.
2. Starten Sie das SafeGuard Management Center auf dem Computer mit dem neu installierten SafeGuard Management Center. Der Konfigurationsassistent wird gestartet und führt Sie durch die notwendigen Schritte.
3. Klicken Sie auf der **Willkommen** Seite auf **Weiter**.
4. Wählen Sie im Dialog **Datenbankverbindung** unter **Datenbankserver** die erforderliche SQL-Datenbankinstanz aus der Liste aus. Alle auf Ihrem Computer oder Netzwerk verfügbaren Datenbankserver werden angezeigt. Wählen Sie unter **Authentisierung** die Art der Authentisierung, die für den Zugriff auf diese Datenbankinstanz benutzt werden soll. Wenn Sie **SQL Server Authentisierung verwenden** wählen, geben Sie die SQL-Benutzerkontenanmeldedaten ein, die Ihr SQL-Administrator erstellt hat. Klicken Sie auf **Weiter**.
5. Aktivieren Sie unter **Datenbankeinstellungen** die Option **Folgende bestehende Datenbank verwenden** und wählen Sie die Datenbank aus der Liste aus. Klicken Sie auf **Weiter**.
6. Wählen Sie unter **SafeGuard Management Center Authentisierung** eine autorisierte Person aus der Liste aus. Wenn Multi Tenancy aktiviert ist, zeigt der Dialog an, welcher Konfiguration sich der Benutzer anmeldet. Geben Sie das Kennwort für den Zertifikatsspeicher ein und bestätigen Sie es.

   Der Zertifikatsspeicher für das aktuelle Benutzerkonto wird angelegt und ist durch dieses abgesichert. Für die nachfolgenden Anmeldungen benötigen Sie nur noch dieses Kennwort.

7. Klicken Sie auf **OK**.

   Eine Meldung, dass Zertifikat und privater Schlüssel nicht gefunden bzw. nicht darauf zugegriffen werden kann, wird angezeigt.

8. Klicken Sie zum Importieren der Daten auf **Ja** und dann auf **OK**. Dadurch wird der Importvorgang gestartet.

9. Klicken Sie unter **Authentisierungs-Schlüsseldatei importieren** auf die [**...**] Schaltfläche und wählen Sie die Schlüsseldatei aus. Geben Sie das **Kennwort der Schlüsseldatei** ein. Geben Sie das zuvor unter **Kennwort des Zertifikatsspeichers oder Token-PIN** definierte Kennwort für den Zertifikatsspeicher ein. Wählen Sie **In den Zertifikatsspeicher importieren** oder **Auf den Token kopieren**, um das Zertifikat auf einem Token zu speichern.
10. Geben Sie zur Initialisierung des Zertifikatsspeichers das Kennwort noch einmal ein.

Zertifikat und privater Schlüssel befinden sich nun im Zertifikatsspeicher. Zur Anmeldung an das SafeGuard Management Center wird das Kennwort des Zertifikatsspeichers verwendet.

6.7 Anmeldung am SafeGuard Management Center

Die Anmeldung richtet sich danach, ob Sie das SafeGuard Management Center im Single Tenancy Modus oder im Multi Tenancy Modus einsetzen.

Informationen zu den ersten Arbeitsschritten im SafeGuard Management Center finden Sie in der SafeGuard Enterprise Administrator-Hilfe.

6.7.1 Anmeldung im Single Tenancy Modus

1. Starten Sie das SafeGuard Management Center über das **Start**-Menü. Ein Anmeldebildschirm wird angezeigt.
2. Melden Sie sich als Haupt-Sicherheitsbeauftragter an und geben Sie das Zertifikatsspeicherkennwort ein, das während der Konfiguration festgelegt wurde. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird gestartet.

Hinweis:

Wenn Sie ein falsches Kennwort eingeben, wird eine Fehlermeldung angezeigt und die nächste Anmeldung wird verzögert. Diese Verzögerung wird mit jedem fehlgeschlagenen Anmeldeversuch größer. Fehlgeschlagene Anmeldeversuche werden protokolliert.

6.7.2 Anmeldung im Multi Tenancy Modus

Wenn Sie mehrere Datenbanken konfiguriert haben (Multi Tenancy), erweitert sich der Anmeldevorgang an das SafeGuard Management Center.

1. Starten Sie das SafeGuard Management Center über den Produktordner im **Start** Menü. Der Dialog **Konfiguration auswählen** wird angezeigt.
2. Wählen Sie die Datenbankkonfiguration, die Sie verwenden möchten, aus der Liste und klicken Sie auf **OK**. Die ausgewählte Datenbankkonfiguration wird mit dem SafeGuard Management Center verbunden und wird aktiv.
3. Sie werden dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird geöffnet und mit der ausgewählten Datenbankkonfiguration verbunden.

Hinweis:

Wenn Sie ein falsches Kennwort eingeben, wird eine Fehlermeldung angezeigt und die nächste Anmeldung wird verzögert. Diese Verzögerung wird mit jedem fehlgeschlagenen Anmeldeversuch größer. Fehlgeschlagene Anmeldeversuche werden protokolliert.

6.8 Einrichten der Organisationsstruktur im SafeGuard Management Center

Es gibt zwei Möglichkeiten, Ihre Organisation in SafeGuard Enterprise abzubilden:

- Directory Service importieren, z. B.: Active Directory

  Während der Synchronisierung mit dem Active Directory werden Objekte (z. B. Computer, Benutzer und Gruppen) in das SafeGuard Management Center importiert und in der SafeGuard Enterprise Datenbank gespeichert.

- Organisationsstruktur manuell aufbauen

  Steht kein Directory Service zur Verfügung oder gibt es nur wenige Organisationseinheiten, so dass kein Directory Service benötigt wird, können Sie neue Domänen/Arbeitsgruppen anlegen, an denen sich der Benutzer/Computer anmelden kann.

Sie können entweder nur eine von beiden Möglichkeiten anwenden, oder die beiden Möglichkeiten mischen. Zum Beispiel können Sie ein Active Directory (AD) ganz oder teilweise importieren und weitere Organisationseinheiten (OU) manuell anlegen. Egal, ob die Organisationsstruktur importiert oder manuell angelegt wird, die Richtlinienzuordnung kann in beiden Fällen erfolgen.

Hinweis:

Beachten Sie, dass bei der Kombination beider Verfahren die manuell angelegten Organisationseinheiten nicht im AD abgebildet werden. Wenn in SafeGuard Enterprise angelegte Organisationseinheiten im AD abgebildet werden sollen, so müssen Sie diese separat zum AD hinzufügen.

Hinweis:

Weitere Informationen zum Importieren oder Anlegen einer Organisationsstruktur finden Sie in der Administrator-Hilfe im Kapitel *Aufbau der Organisationsstruktur*.

6.9 Importieren der Lizenzdatei

SafeGuard Enterprise hat einen integrierten Lizenzzähler. Die Installation umfasst standardmäßig für jedes SafeGuard Enterprise Modul eine festgelegte Anzahl von 5 Lizenzen. Dadurch soll eine problemlose Evaluierung von anderen SafeGuard Enterprise Modulen ohne Nebeneffekte gewährleistet werden. Beim Kauf von SafeGuard Enterprise enthält jedoch jeder Kunde eine individuelle Lizenzdatei für das jeweilige Unternehmen, die in das SafeGuard Management Center importiert werden muss.

Weitere Informationen finden Sie in der Administrator-Hilfe im Kapitel *Lizenzen*.

6.10 Wiederherstellen einer beschädigten SafeGuard Enterprise Installation

Eine beschädigte SafeGuard Management Center Installation kann auf einfache Art und Weise wiederhergestellt werden, wenn die Datenbank noch intakt ist. In diesem Fall müssen Sie nur das SafeGuard Management Center neu installieren und die vorhandene Datenbank sowie das gesicherte Sicherheitsbeauftragten-Zertifikat verwenden.

- Das Unternehmenszertifikat und das Haupt-Sicherheitsbeauftragten-Zertifikat der betreffenden Datenbankkonfiguration müssen als .p12 Dateien exportiert worden sein. Die Dateien müssen vorhanden und gültig sein.
- Die Kennwörter für die .p12 Dateien sowie für den Zertifikatsspeicher müssen Ihnen bekannt sein.

So stellen Sie eine beschädigte SafeGuard Management Center Installation wieder her:

1. Installieren Sie das SafeGuard Management Center Installationspaket neu. Öffnen Sie das SafeGuard Management Center. Der Konfigurationsassistent wird automatisch geöffnet.
2. Wählen Sie unter **Datenbankverbindung** den relevanten Datenbankserver und konfigurieren Sie, falls erforderlich, die Verbindung zur Datenbank. Klicken Sie auf **Weiter**.
3. Aktivieren Sie unter **Datenbankeinstellungen** die Option **Folgende bestehende Datenbank verwenden** und wählen Sie die Datenbank aus der Liste aus.
4. Führen Sie unter **Daten des Sicherheitsbeauftragten** einen der folgenden Schritte aus:
   - Wenn die gesicherte Zertifikatsdatei auf dem Computer gefunden wird, wird sie angezeigt. Geben Sie das Kennwort ein, das Sie zur Anmeldung an das SafeGuard Management Center benutzen.
   - Wird die gesicherte Zertifikatsdatei nicht auf dem Computer gefunden, wählen Sie **Importieren**. Suchen Sie nach der gesicherten Zertifikatsdatei und klicken Sie auf **Öffnen**. Geben Sie das Kennwort für die Zertifikatsdatei ein. Klicken Sie auf **Ja**. Geben Sie ein Kennwort für die Anmeldung am SafeGuard Management Center ein und bestätigen Sie es.
5. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um die Konfiguration des SafeGuard Management Center abzuschließen.

Die SafeGuard Management Center Installation ist wiederhergestellt.

6.11 Wiederherstellen einer beschädigten Datenbankkonfiguration

Sie können eine korrupte Datenbankkonfiguration wiederherstellen, indem Sie das SafeGuard Management Center neu installieren und basierend auf den gesicherten Zertifikatsdateien eine neue Instanz der Datenbank erstellen. Dadurch wird sichergestellt, dass alle vorhandenen SafeGuard Enterprise Endpoint-Computer Richtlinien von der neuen Installation annehmen. Somit müssen Sie nicht die gesamte Datenbank neu einrichten und wiederherstellen.

- Das Unternehmenszertifikat und das Haupt-Sicherheitsbeauftragten-Zertifikat der betreffenden Datenbankkonfiguration müssen als .p12 Dateien exportiert worden sein. Die Dateien müssen vorhanden und gültig sein. Erstellen Sie Zertifikate-Backups im

SafeGuard Management Center. Weitere Informationen finden Sie in der Administrator-Hilfe.

- Die Kennwörter für die beiden .p12 Dateien sowie für den Zertifikatsspeicher müssen Ihnen bekannt sein.

So stellen Sie eine korrupte Datenbank wieder her:

1. Installieren Sie das SafeGuard Management Center Installationspaket neu. Öffnen Sie das SafeGuard Management Center. Der Konfigurationsassistent wird automatisch geöffnet.
2. Wählen Sie unter **Datenbank-Verbindung** die Option **Neue Datenbank erstellen**. Konfigurieren Sie unter **Datenbankeinstellungen** die Verbindung zur Datenbank. Klicken Sie auf **Weiter**.
3. Wählen Sie unter **Daten des Sicherheitsbeauftragten** den relevanten Haupt-Sicherheitsbeauftragten und klicken Sie auf **Importieren**.
4. Suchen Sie unter **Importieren des Zertifikats** die gesicherte Schlüsseldatei. Geben Sie unter **Kennwort der Datei** das für diese Datei festgelegte Kennwort ein und bestätigen Sie es. Wählen Sie **Schlüsseldatei im Zertifikatsspeicher speichern** und geben Sie das Kennwort für den Speicher ein. Klicken Sie auf **OK**.
5. Das Zertifikat des Haupt-Sicherheitsbeauftragten wird importiert. Klicken Sie auf **Weiter**.
6. Aktivieren Sie unter **Unternehmenszertifikat** die Option **Über vorhandenes Unternehmenszertifikat wiederherstellen**. Klicken Sie auf **Importieren**, um die gesicherte Zertifikatsdatei auszuwählen, die das gültige Unternehmenszertifikat enthält. Sie werden aufgefordert, das für den Zertifikatsspeicher definierte Kennwort einzugeben. Geben Sie das Kennwort ein und klicken Sie auf **OK**. Bestätigen Sie die angezeigte Meldung mit **Ja**. Das Unternehmenszertifikat wird importiert.
7. Klicken Sie auf **Weiter**, dann auf **Beenden**.

Die Datenbankkonfiguration ist wiederhergestellt.

7 Testen der Kommunikation

Wenn SafeGuard Enterprise Server, die Datenbank und das SafeGuard Management Center eingerichtet sind, sollten Sie einen Verbindungstest durchführen. Die nötigen Schritte werden in diesem Kapitel beschrieben.

7.1 Voraussetzungen

Vor dem Verbindungstest müssen folgende Einstellungen gemacht bzw. geprüft werden:

7.1.1 Ports/Verbindungen

Die Endpoint-Computer müssen folgende Verbindungen aufbauen:

SafeGuard Client Verbindung zu	Port
SafeGuard Enterprise Server	Port 80/TCP Port 443 bei Benutzung der SSL Transportverbindung

Das SafeGuard Management Center muss folgende Verbindungen aufbauen:

SafeGuard Management Center Verbindung zu	Port
SQL Datenbank	SQL Server 2005/SQL Server 2008 dynamischer Port: Port 1433/TCP und Port 1434/TCP
Active Directory	Port 389/TCP
SLDAP	Port 636 für den Active Directory Import

Der SafeGuard Enterprise Server muss folgende Verbindungen aufbauen:

SafeGuard Enterprise Server Verbindung zu	Port
SQL Datenbank	Port 1433/TCP und Port 1434/TCP für SQL 2005 (Express) dynamic port
Active Directory	Port 389/TCP

7.1.2 Authentisierungsmethode

1. Öffnen Sie auf dem Computer, auf dem SafeGuard Enterprise Server installiert ist, den **Internet Information Services (IIS) Manager**.
2. Klicken Sie in der Baumstruktur auf **Internet Information Services Manager.** Klicken Sie auf **Servername**, **Websites**, **Standard-Website**.
3. Klicken Sie mit der rechten Maustaste auf **SGNSRV** und klicken Sie auf **Eigenschaften.**
4. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**.
5. Klicken Sie unter **Authentifizierung und Zugriffssteuerung** auf **Bearbeiten**. In **Authentifizierungsverfahren** wählen Sie **Anonymen Zugriff aktivieren**. Deaktivieren Sie unter **Authentifizierter Zugriff** das Kontrollkästchen **Integrierte Windows-Authentifizierung**.

7.1.3 Proxyserver-Einstellungen für Webserver und Endpoint-Computer

Definieren Sie die Proxyserver-Einstellungen wie folgt:

1. Klicken Sie im Internet Explorer im **Extras** Menü auf **Internetoptionen**. Klicken Sie auf **Verbindungen** und dann auf **LAN-Einstellungen**.
2. Deaktivieren Sie in **LAN-Einstellungen** unter **Proxyserver** das Kontrollkästchen **Proxyserver für LAN verwenden**.

   Wenn ein Proxyserver notwendig ist, wählen Sie **Proxyserver für lokale Adressen umgehen**.

7.1.4 Microsoft SQL Server 2005 Einstellungen

Wenn Sie Microsoft SQL Server 2005 verwenden, nehmen Sie die folgenden Einstellungen vor:

1. Öffnen Sie Microsoft SQL Server Management Studio.
2. Klicken Sie im linken Bereich des **Object Explorer** auf **Sicherheit.**
3. Klicken Sie mit der rechten Maustaste auf **Anmeldungen** und klicken Sie auf **Neue Anmeldung**. Fügen Sie in Microsoft SQL Server Management Studio folgenden Benutzer (Rolle "sysadmin") hinzu: **NT AUTHORITY\NETWORK SERVICE**.

7.2 Testen Der Verbindung (IIS 6 auf Windows Server 2003)

1. Öffnen Sie auf dem Computer, auf dem SafeGuard Enterprise Server installiert ist, den **Internet Information Services (IIS) Manager**.
2. Klicken Sie in der Baumstruktur auf **Internet Information Services Manager**. Klicken Sie auf **Servername**, **Websites**, **Standard-Website**. Überprüfen Sie, ob die Web-Seite **SGNSRV** im Ordner **Standard-Web-Seite** verfügbar ist.
3. Klicken Sie mit der rechten Maustaste auf **SGNSRV** und klicken Sie auf **Durchsuchen**. Auf der rechten Seite des Fensters wird eine Liste mit möglichen Aktionen angezeigt.

4. Wählen Sie aus dieser Liste die Aktion **Verbindung prüfen**. Die mögliche Aktion wird auf der rechten Seite des Fensters angezeigt.
5. Um die Verbindung zu prüfen, klicken Sie auf **Aufrufen**.

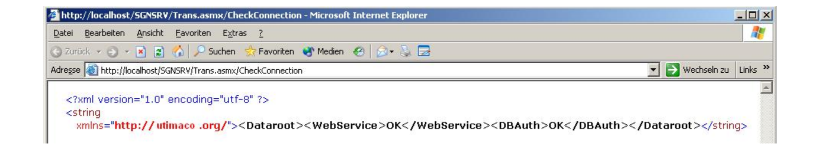
Der Verbindungstest war erfolgreich, wenn Sie diese Ausgabe erhalten:



7.3 Testen der Verbindung (IIS 7 auf Windows Server 2008)

1. Öffnen Sie auf dem Computer, auf dem SafeGuard Enterprise Server installiert ist, den **Internet Information Services (IIS) Manager**.
2. Klicken Sie in der Baumstruktur auf **"Servername"**, **Websites**, **Standard-Website**. Überprüfen Sie, ob die Web-Seite **SGNSRV** im Ordner **Standard-Website** verfügbar ist.
3. Klicken Sie mit der rechten Maustaste auf **SGNSRV**, wählen Sie **Anwendung** und klicken Sie **Browse**, um die **SGNSRV Homepage Sophos SafeGuard Web Service** zu öffnen.
4. Auf der **Sophos SafeGuard Web Service** Seite wird eine Liste mit möglichen Aktionen angezeigt. Klicken Sie in dieser Liste auf die Aktion **CheckConnection**.
5. Klicken Sie auf der **CheckConnection** Seite auf **Aufrufen**.

Der Verbindungstest war erfolgreich, wenn Sie diese Ausgabe erhalten:



8 Registrieren und Konfigurieren des SafeGuard Enterprise Servers

Zur Implementierung der Informationen für die Kommunikation zwischen IIS Server, Datenbank und SafeGuard Client muss der SafeGuard Enterprise Server registriert und konfiguriert werden. Die Informationen werden in einem Server-Konfigurationspaket (MSI) gespeichert.

Diesen Schritt führen Sie im SafeGuard Management Center aus. Der Workflow ist davon abhängig, ob der SafeGuard Enterprise Server auf demselben Computer wie das SafeGuard Management Center oder auf einem anderen Computer installiert ist.

Sie können auch weitere Eigenschaften festlegen. So lassen sich z. B. zusätzliche Sicherheitsbeauftragte für den ausgewählten Server hinzufügen. Sie können auch die Verbindung zur Datenbank konfigurieren.

8.1 Registrieren und Konfigurieren des SafeGuard Enterprise Server für die Benutzung auf dem aktuellen Computer

Nachdem Sie das SafeGuard Management Center und SafeGuard Enterprise Server auf dem Computer, mit dem Sie derzeit arbeiten, installiert haben, registrieren und konfigurieren Sie den SafeGuard Enterprise Server.

Hinweis:

Wenn Multi Tenancy installiert ist, steht diese Option nicht zur Verfügung.

1. Starten Sie das SafeGuard Management Center.
2. Klicken Sie im **Extras** Menü auf **Konfigurationspakete**.
3. Wählen Sie die Registerkarte **Server registrieren** und klicken Sie auf **Diesen Computer zum SGN Server machen**.
4. Wählen Sie die Registerkarte **Server registrieren** und klicken Sie auf **Optionen**:

   Das SafeGuard Enterprise Server Configuration Setup wird automatisch gestartet.

5. Übernehmen Sie in allen folgenden Dialogen die Standardeinstellungen.

Der SafeGuard Enterprise Server ist installiert. Ein Server-Konfigurationspaket mit der Bezeichnung <**Server**>**.msi** wird erstellt und direkt auf dem aktuellen Computer installiert. Die Serverinformationen werden in der Registerkarte **Server registrieren** angezeigt. Sie können zusätzliche Konfigurationsschritte durchführen.

Hinweis:

Wenn Sie ein neues Server-Konfigurationspaket (MSI) auf dem SafeGuard Enterprise Server installieren möchten, deinstallieren Sie zunächst das veraltete Konfigurationspaket. Löschen Sie darüber hinaus den Local Cache manuell, so dass er mit den neuen Konfigurationsdaten (z. B. SSL-Einstellungen) aktualisiert werden kann. Installieren Sie dieses Konfigurationspaket auf dem Server.

8.2 Registrieren und Konfigurieren des SafeGuard Enterprise Servers für die Benutzung auf einem anderen Computer

Wenn der SafeGuard Enterprise Server auf einem anderen Computer als das SafeGuard Management Center installiert wurde, registrieren und konfigurieren Sie den SafeGuard Enterprise Server:

1. Starten Sie das SafeGuard Management Center.
2. Klicken Sie im **Extras** Menü auf **Konfigurationspakete**.
3. Wählen Sie die Registerkarte **Server registrieren** und klicken Sie auf **Hinzufügen**.
4. Klicken Sie unter **Serverregistrierung** auf die Schaltfläche [**...**], um das Maschinenzertifikat des Servers auszuwählen. Es wird bei der Installation des SafeGuard Enterprise Servers erzeugt. Sie finden es standardmäßig im Verzeichnis **MachCert** des SafeGuard Enterprise Server Installationsverzeichnisses. Es trägt den Dateinamen <**Computername**>**.cer**. Wenn der SafeGuard Enterprise Server auf einem anderen Computer als das SafeGuard Management Center installiert ist, muss diese .cer-Datei als Kopie oder Netzwerkfreigabe zugreifbar sein.

   Wählen Sie nicht das MSO-Zertifikat.

   Der Fully Qualified Name (FQDN), z. B. **server.mycompany.edu**, sowie Zertifikatsinformationen werden angezeigt.

   Hinweis:

   Wenn SSL als Tansportverschlüsselung zwischen Client und Server verwendet werden soll, muss der Servername, den Sie hier eingeben mit dem Servernamen übereinstimmen, den Sie im SSL-Zertifikat vergeben haben. Andernfalls können Client und Server nicht miteinander kommunizieren.

5. Klicken Sie auf **OK**.

   Die Serverinformationen werden in der Registerkarte **Server registrieren** angezeigt.

6. Klicken Sie auf die Registerkarte **Server-Konfigurationspaket erstellen**. Hier werden alle verfügbaren Server angezeigt. Wählen Sie dort den gewünschten Server aus. Geben Sie einen Ausgabepfad für das Konfigurationspaket an. Klicken Sie auf **Konfigurationspaket erstellen**.

   Ein Server-Konfigurationspaket (MSI) mit der Bezeichnung <**Server**>**.msi** wird im angegebenen Ausgabeort erstellt.

7. Bestätigen Sie die Erfolgsmeldung mit **OK**.
8. Klicken Sie in der Registerkarte **Server registrieren** auf **Schließen**.

Die Registrierung und Konfiguration des SafeGuard Enterprise Servers ist beendet. Installieren Sie das Server-Konfigurationspaket (MSI) auf dem Computer, auf dem der SafeGuard Enterprise Server läuft. Sie können die Serverkonfiguration in der Registerkarte **Server registrieren** jederzeit ändern.

Hinweis:

Wenn Sie ein neues Server-Konfigurationspaket (MSI) auf dem SafeGuard Enterprise Server installieren möchten, deinstallieren Sie zunächst das veraltete Konfigurationspaket. Löschen Sie darüber hinaus den Local Cache manuell, so dass er mit den neuen Konfigurationsdaten (z. B. SSL-Einstellungen) aktualisiert werden kann. Installieren Sie dieses Konfigurationspaket auf dem Server.

8.3 Ändern der SafeGuard Enterprise Server Konfigurationseinstellungen

Sie können die Eigenschaften und Einstellungen für jeden registrierten Server und seine Datenbankverbindung jederzeit ändern.

1. Wählen Sie den gewünschten Server in der Registerkarte **Server registrieren** des SafeGuard Management Center **Konfigurationspakete** Werkzeugs.
2. Gehen Sie wie folgt vor:

Element	Beschreibung
Skripts ausführen	Klicken Sie hier, um die Verwendung von SafeGuard Enterprise API zu ermöglichen. Dies ermöglicht die Ausführung von administrativen Aufgaben über Skripts.
Server-Rollen	Klicken Sie hier, um eine verfügbare Sicherheitsbeauftragtenrolle für den ausgewählten Server zu aktivieren/deaktivieren.
Server-Rolle hinzufügen...	Klicken Sie hier, um weitere spezifische Sicherheitsbeauftragtenrollen für den ausgewählten Server hinzuzufügen, falls erforderlich. Sie werden dazu aufgefordert, das Serverzertifikat auszuwählen. Die Sicherheitsbeauftragtenrolle wird hinzugefügt und kann unter **Server-Rollen** angezeigt werden.
Datenbankverbindung	Klicken Sie auf **[...]**, um die Verbindung zur Datenbank für jeden registrierten Server zu konfigurieren. Hier können Sie auch die Anmeldeinformationen für die Datenbank und die Transportverschlüsselung zwischen Web Server und Datenbankserver festlegen. Für weitere Informationen, *siehe Konfigurieren der Datenbankserver-Verbindung* (Seite 35). Selbst wenn die Prüfung der Datenbankverbindung nicht erfolgreich ist, kann ein neues Server-Konfigurationspaket erstellt werden. **Hinweis:** Sie müssen nicht den SafeGuard Management Center Konfigurationsassistenten erneut ausführen, um die Datenbankkonfiguration zu aktualisieren. Sie müssen nur dafür sorgen, ein neues Server-Konfigurationspaket zu erstellen und es an den entsprechenden Server zu verteilen. Sobald dieses auf dem Server installiert ist, kann auf die neue Datenbankverbindung zugegriffen werden.

3. Erstellen Sie ein neues Server-Konfigurationspaket in der Registerkarte **Server-Konfigurationspaket erstellen**.

4. Deinstallieren Sie das veraltete Server-Konfigurationspaket und installieren Sie danach das neue auf dem entsprechenden Server.

Die neue Server-Konfiguration wird aktiv.

8.4 Registrieren des SafeGuard Enterprise Servers mit aktivierter Sophos Firewall

Ein SafeGuard Enterprise Client kann keine Verbindung mit dem SafeGuard Enterprise Server herstellen, wenn eine Sophos Firewall mit Standardeinstellungen auf dem Endpoint-Computer installiert ist. Die Sophos Firewall sperrt standardmäßig NetBIOS-Verbindungen, die für die Auflösung des Netzwerknamens des SafeGuard Enterprise Servers benötigt werden.

1. Führen Sie als Workaround einen der folgenden Schritte aus:
   - Geben Sie die NetBIOS-Verbindungen in der Firewall frei.
   - Fügen Sie den Fully Qualified Name des SafeGuard Enterprise Servers im Konfigurationspaket hinzu. Für weitere Informationen, *siehe Registrieren und Konfigurieren des SafeGuard Enterprise Servers für die Benutzung auf einem anderen Computer* (Seite 50).

9 SafeGuard Enterprise auf Endpoint-Computern einrichten

SafeGuard Enterprise fügt sich nahtlos in die gewohnte Benutzerumgebung ein und lässt sich leicht und intuitiv bedienen. Je nach Ihrer Strategie für den Einsatz von SafeGuard Enterprise können Sie die Endpoint-Computer mit verschiedenen SafeGuard Enterprise Modulen ausstatten und sie gemäß Ihren Anforderungen konfigurieren.

Sicherheitsbeauftragte können die Installation und Konfiguration lokal auf den Endpoint-Computern oder im Rahmen einer zentralisierten Software-Installation ausführen. Durch das zentrale Einrichten von Endpoint-Computern wird eine standardisierte Installation auf mehreren Computern erreicht.

9.1 SafeGuard Konfigurationen für Endpoint-Computer

Endpoint-Computer können folgendermaßen konfiguriert werden:

- **SafeGuard Enterprise Clients (managed)**

  Zentrale, Server-basierte Verwaltung im SafeGuard Management Center

  Für SafeGuard Enterprise Clients (managed) besteht generell eine Verbindung zum SafeGuard Enterprise Server. Sie erhalten ihre Richtlinien über den SafeGuard Enterprise Server. Die Verbindung kann temporär unterbrochen sein, z. B. während einer Geschäftsreise. Trotzdem ist der Endpoint-Computer auch in dieser Situation als SafeGuard Enterprise Client definiert.

- **Sophos SafeGuard Standalone Clients**

  Lokale Verwaltung im SafeGuard Management Center

  Für Sophos SafeGuard Clients (standalone) besteht nie eine Verbindung zum SafeGuard Enterprise Server. Damit fehlt die Verbindung zur zentralen Verwaltung von SafeGuard Enterprise. Er wird im Standalone-Modus betrieben.

  Der zentrale Unterschied zum SafeGuard Enterprise Client (managed) ist, dass Sophos SafeGuard Clients (standalone) SafeGuard Enterprise Richtlinien ausschließlich über ein Konfigurationspaket erhalten. Diese Computer erhalten Richtlinien nie über eine Verbindung zum SafeGuard Enterprise Server.

  SafeGuard Enterprise Richtlinien werden im SafeGuard Management Center erstellt und in Konfigurationspakete exportiert. Die Verteilung der Konfigurationspakete kann über firmeneigene Software-Verteilungsmechanismen erfolgen, oder das Konfigurationspaket wird manuell auf den Endpoint-Computern installiert.

9.1.1 Installationspakete für SafeGuard Enterprise Clients (managed)

Hinweis:

Wenn das Betriebssystem des Endpoint-Computers Windows 7 64-Bit oder Windows Vista 64-Bit ist, können Sie die 64-Bit-Variante der “Client” Installationspakete

(<Paketname>_x64.msi) installieren. Das 64-Bit Paket des Configuration Protection Client ist für Windows 7 64 Bit verfügbar.

Die folgende Tabelle zeigt die für SafeGuard Enterprise Clients (managed) verfügbaren Installationspakete.

Paket	Beschreibung
SGxClientPreinstall.msi	Muss vor der Verschlüsselungssoftware auf den Endpoint-Computern installiert werden (obligatorisch). Stattet Endpoint-Computer mit notwendigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware aus.
SGNClient.msi SGNClient_x64.msi	Für SafeGuard Enterprise Clients und für SafeGuard Enterprise Clients mit BitLocker-Unterstützung. **SafeGuard Enterprise Device Encryption** Volume-basierende Verschlüsselung mit Power-on Authentication. **SafeGuard Data Exchange** Einfacher Datenaustausch mit Wechselmedien auf allen Plattformen ohne Neuverschlüsselung. Dateibasierende Verschlüsselung
SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi	Für SafeGuard Enterprise Clients mit BitLocker-Unterstützung steht dieses Paket nicht zur Verfügung. **SafeGuard Data Exchange** Einfacher Datenaustausch mit Wechselmedien auf allen Plattformen ohne Neuverschlüsselung. Dateibasierende Verschlüsselung ohne Power-on Authentication
SGN_CP_Client.msi SGN_CP_Client_x64.msi	Für SafeGuard Enterprise Clients und für SafeGuard Enterprise Clients mit BitLocker-Unterstützung. Die 64-Bit-Variante dieses Pakets ist für Windows 7 64-Bit Betriebssysteme verfügbar. **Configuration Protection** Schnittstellenschutz und Management von Peripheriegeräten
SGNClientRuntime.msi SGNClientRuntime_x64.msi	Runtime Client, der das Starten des Computers von einem sekundären Boot-Volume ermöglicht, wenn mehrere Betriebssysteme installiert sind. Zugriff auf diese Volumes, wenn sie auf dem primären Volume durch eine SafeGuard Enterprise Installation verschlüsselt sind.

9.1.2 Installationspakete für Sophos SafeGuard Clients (standalone)

Hinweis:

Wenn das Betriebssystem des Endpoint-Computers Windows 7 64-Bit oder Windows Vista 64-Bit ist, können Sie die 64-Bit-Variante der “Client” Installationspakete (<Paketname>_x64.msi) installieren.

Die folgende Tabelle zeigt die für Sophos SafeGuard Clients (standalone) verfügbaren Installationspakete.

Paket	Beschreibung
SGxClientPreinstall.msi	Muss vor der Verschlüsselungssoftware auf den Endpoint-Computern installiert werden (obligatorisch). Stattet Endpoint-Computer mit notwendigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware aus.
SGNClient.msi SGNClient_x64.msi	**SafeGuard Enterprise Device Encryption** Volume-basierende Verschlüsselung mit Power-on Authentication. **SafeGuard Data Exchange** Einfacher Datenaustausch mit Wechselmedien auf allen Plattformen ohne Neuverschlüsselung. Dateibasierende Verschlüsselung
SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi	**SafeGuard Data Exchange** Einfacher Datenaustausch mit Wechselmedien auf allen Plattformen ohne Neuverschlüsselung. Dateibasierende Verschlüsselung ohne Power-on Authentication
SGNClientRuntime.msi SGNClientRuntime_x64.msi	Runtime Client, der das Starten des Computers von einem sekundären Boot-Volume ermöglicht, wenn mehrere Betriebssysteme installiert sind. Zugriff auf diese Volumes, wenn sie auf dem primären Volume durch eine SafeGuard Enterprise Installation verschlüsselt sind.

9.2 Einschränkungen

Beachten Sie die in den folgenden Abschnitten beschriebenen Einschränkungen für SafeGuard Enterprise auf Endpoint-Computern.

9.2.1 Allgemeine Einschränkungen

Beachten Sie folgende allgemeine Einschränkungen für SafeGuard Enterprise Clients:

- SafeGuard Enterprise for Windows unterstützt keine Apple Hardware und kann nicht in einer Bootcamp-Umgebung installiert werden.

- Wenn auf dem Computer Intel Advanced Host Controller Interface (AHCI) benutzt wird, so muss sich die Boot-Festplatte in Slot 0 oder Slot 1 befinden. Sie können bis zu 32 Festplatten einlegen. SafeGuard Enterprise läuft nur auf den ersten beiden Slot-Nummern.
- Volume-basierende Verschlüsselung für dynamische Festplatten und GUID Partitionstabellen (GPT)-Platten werden nicht unterstützt. Die Installation bricht in diesem Fall ab. Wenn diese Platten nachträglich im System auftauchen, werden sie nicht unterstützt.
- Systeme mit Festplatten, die über einen SCSI Bus angeschlossen sind, werden vom SafeGuard Enterprise Device Encryption Modul nicht unterstützt.

9.2.2 Einschränkungen für SafeGuard Enterprise Clients (managed)

Beachten Sie die folgenden Einschränkungen für die Initialverschlüsselung von SafeGuard Enterprise Clients (managed).

- Einschränkungen für die Initialverschlüsselung

  Im Rahmen der initialen Konfiguration von SafeGuard Enterprise Clients (managed) können Verschlüsselungsrichtlinien erstellt werden, die in einem Konfigurationspaket an die SafeGuard Enterprise Clients verteilt werden können.

  Wenn der SafeGuard Enterprise Client jedoch nicht direkt nach der Installation des Konfigurationspakets eine Verbindung mit dem SafeGuard Enterprise Server herstellt, sondern vorübergehend offline ist, werden nur Verschlüsselungsrichtlinien mit den folgenden spezifischen Einstellungen sofort auf dem SafeGuard Enterprise Client wirksam:

  Geräteschutz vom Typ volume-basierend unter Anwendung des definierten Computerschlüssels als Verschlüsselungsschlüssel

  Damit alle anderen Richtlinien, die Verschlüsselung mit benutzerdefinierten Schlüsseln umfassen, auf dem SafeGuard Enterprise Client aktiv werden, muss das entsprechende Konfigurationspaket auch noch einmal der OU (Organizational Unit) des Clients zugewiesen werden. Die benutzerdefinierten Schlüssel werden dann erst erstellt, wenn der SafeGuard Enterprise Client wieder eine Verbindung zum SafeGuard Enterprise Server hergestellt hat.

  Ursache hierfür ist, dass der definierte Computerschlüssel direkt auf dem SafeGuard Enterprise Client beim ersten Neustart nach der Installation erstellt wird. Benutzerdefinierte Schlüssel hingegen können nur auf dem SafeGuard Enterprise Client erstellt werden, wenn er beim SafeGuard Enterprise Server registriert wurde.

- Einschränkungen für die Unterstützung von BitLocker Device Encryption:

  Die Installationspakete SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi stehen für die Anwendung mit BitLocker Device Encryption nicht zur Verfügung.

  Hinweis:

  Unter Windows Vista oder Windows 7 kann jeweils nur die volume-basierende Verschlüsselung von SafeGuard Enterprise oder BitLocker Device Encryption verwendet werden. Die gleichzeitige Verwendung beider Verschlüsselungstypen ist nicht möglich. Wenn Sie den Verschlüsselungstyp ändern möchten, müssen Sie zuerst alle Partitionen entschlüsseln, das SafeGuard Enterprise Client-Paket deinstallieren und dann mit den gewünschten Features neu installieren. Wenn Sie versuchen, beide Features gleichzeitig zu installieren, wird die Installation abgebrochen.

9.2.3 Einschränkungen für Sophos SafeGuard Clients (standalone)

Die folgende Features werden für Sophos SafeGuard Clients (standalone) nicht unterstützt:

- BitLocker Device Encryption, BitLocker To Go
- Configuration Protection

9.3 Vorbereiten der Verschlüsselung

Vor der Installation von SafeGuard Enterprise empfehlen wir folgende vorbereitende Maßnahmen.

- Führen Sie die allgemeinen vorbereitenden Maßnahmen durch, *siehe Vorbereiten der Installation* (Seite 13).
- Auf den Endpoint-Computern muss ein Benutzerkonto eingerichtet und aktiv sein.
- Erstellen Sie einen kompletten Backup Ihrer Daten auf dem Endpoint-Computer.
- Sophos stellt eine Liste für die Hardware-Konfiguration zur Verfügung, um Konflikte zwischen der POA und Ihrer Computerhardware zu vermeiden. Die Liste ist im Installationspaket der Verschlüsselungssoftware enthalten.

  Wir empfehlen, vor jeder größer angelegten SafeGuard Enterprise Installation die aktuelle Version der POA-Konfigurationsdatei zu installieren. Die Datei wird monatlich aktualisiert und steht hier zum Download zur Verfügung: *ftp://POACFG:POACFG@ftp.ou.utimaco.de*

  Sie können uns bei der Optimierung der Hardware-Kompatibilität unterstützen, indem Sie ein von uns zur Verfügung gestelltes Tool ausführen. Dieses Tool liefert ausschließlich Hardware-relevante Informationen. Das Tool ist einfach zu bedienen. Die gesammelten Informationen werden zur Hardware-Konfigurationsdatei hinzugefügt.

  Für weitere Informationen, siehe
  http://www.sophos.de/support/knowledgebase/article/110285.html und
  http://www.sophos.de/support/knowledgebase/article/65700.html.
- Untersuchen Sie die Festplatte(n) mit folgendem Kommando auf Fehler:

  chkdsk %drive% /F /V /X

  Unter Umständen werden Sie dazu aufgefordert, den Computer neu zu starten und **chkdsk** noch einmal auszuführen. Weitere Informationen finden Sie hier:
  http://www.sophos.de/support/knowledgebase/article/107799.html

  Die Ergebnisse (Log-Datei) können Sie in der Windows-Ereignisanzeige prüfen.

    Windows XP: Wählen Sie **Anwendung**, **Winlogon**.
    Windows 7, Windows Vista: Wählen Sie **Windows Logs**, **Anwendung**, **Wininit**.

- Benutzen Sie das Windows-Tool defrag, um fragmentierte Boot-Dateien, Datendateien und Ordner auf lokalen Volumes aufzufinden und zu konsolidieren. Weitere Informationen finden Sie hier: *http://www.sophos.de/support/knowledgebase/article/109226.html*.
- Deinstallieren Sie Third-Party Boot-Manager, z. B. PROnetworks Boot Pro und Boot-US.

- Wenn Sie Image/Clone-Programme verwendet haben, empfehlen wir, den MBR neu zu schreiben. Für die Installation von Sophos SafeGuard benötigen Sie einen sauberen, einwandfreien Master Boot Record. Möglicherweise ist der MBR aber durch den Einsatz von Imaging/Cloning-Programmen nicht mehr in einwandfreiem, ursprünglichen Zustand.

  Sie können den Master Boot Record säubern, indem Sie von einer Windows-DVD booten und den Befehl **FIXMBR** innerhalb der Windows Recovery Console ausführen. Weitere Informationen finden Sie hier:
  http://www.sophos.de/support/knowledgebase/article/108088.html.

- Wenn die Bootpartition von FAT nach NTFS konvertiert wurde, der Computer aber noch nicht neu gestartet wurde, installieren Sie SafeGuard Enterprise nicht. Möglicherweise wird die Installation nicht beendet, da das Dateisystem zum Zeitpunkt der Installation noch FAT ist, jedoch zum Zeitpunkt der Aktivierung NTFS vorgefunden wird. In diesem Fall müssen Sie den Computer einmalig neu starten, bevor SafeGuard Enterprise installiert wird.

- Nur für SafeGuard Enterprise Clients (managed): Kontrollieren Sie, ob eine Verbindung zum SafeGuard Enterprise Server besteht. Rufen Sie auf den Endpoint-Computern im Internet Explorer folgende Web-Adresse auf: http://<ServerIPAddress>/sgnsrv. Wenn die **Trans**-Seite mit dem Eintrag **Check Connection** erscheint, ist die Verbindung zum SafeGuard Enterprise Server hergestellt. Für weitere Informationen, *siehe Testen Der Verbindung (IIS 6 auf Windows Server 2003)* (Seite 47).

9.3.1 Spezifische vorbereitende Maßnahmen für die Unterstützung von BitLocker Device Encryption

Hinweis:

Entscheiden Sie vor der Installation, ob Sie SafeGuard Enterprise in Verbindung mit der BitLocker Drive Encryption oder die volume-basierende Verschlüsselung von SafeGuard Enterprise anwenden möchten.
Wenn Sie versuchen, beides gleichzeitig zu installieren, wird die Installation abgebrochen.

Wenn Sie mit SafeGuard Enterprise BitLocker Endpoint-Computer verwalten möchten, sind folgende spezifische vorbereitende Maßnahmen auf dem Endpoint-Computer zu treffen.

- Auf dem Endpoint-Computer muss Windows Vista Enterprise oder Ultimate oder Windows 7 installiert sein.
- Es muss eine zweite Partition für das BitLocker System-Volume mit einer NTFS-formatierte Klartextpartition mit mindestens 1.5 GB vorhanden sein. Microsoft bietet ein BitLocker Partitionierungs-Tool.
- BitLocker Device Encryption muss installiert und aktiviert sein.
- Wenn TPM für die Authentisierung verwendet werden soll, muss TPM initialisiert, im Besitz und aktiviert sein.
- Wenn Sie die volume-basierende Verschlüsselung von SafeGuard Enterprise installieren möchten, sollten Sie sicherstellen, dass die Volumes nicht bereits mit BitLocker Drive Encryption verschlüsselt wurden. Andernfalls kann es zu einer Beschädigung des Systems kommen.

- Um die BitLocker Drive Encryption Unterstützung zu installieren, deaktivieren Sie entweder User Access Control (UAC) oder melden Sie sich mit dem integrierten Administrator-Benutzerkonto an.

Weitere Informationen erhalten Sie vom Microsoft Support oder auf den folgenden Websites:

- Vorbereitung für BitLocker:

  http://technet2.microsoft.com/WindowsVista/en/library/c61f2a12-8ae6-4957-b031-97b4d762cf311033.mspx?mfr=true

- BitLocker FAQ:

  http://technet2.microsoft.com/WindowsVista/en/library/58358421-a7f5-4c97-ab41-2bcc61a58a701033.mspx?mfr=true

9.3.2 Vorbereiten einer "Ändern"-Installation

Wenn Sie eine vorhandene SafeGuard Enterprise Installation ändern oder bestimmte Module zu einem späteren Zeitpunkt installieren, meldet das Installationsprogramm u. U., dass bestimmte Komponenten (z. B. SafeGuard Removable Media Manager) derzeit benutzt werden. Diese Meldung wird dadurch verursacht, dass diese Module gemeinsame Komponenten benutzen, die derzeit verwendet werden und daher nicht sofort aktualisiert werden können. Diese Meldung kann ignoriert werden, da die betroffenen Komponenten beim Neustart des Computers ohnehin aktualisiert werden.

Dieses Verhalten gilt für die Installation in überwachtem und nicht überwachtem Modus.

9.4 Erstellen von Konfigurationspaketen - Überblick

Erstellen Sie je nach erforderlicher Konfiguration spezifische Konfigurationspakete für die Endpoint-Computer im SafeGuard Management Center:

- Für SafeGuard Enterprise Clients (managed)
- Für Sophos SafeGuard Standalone Clients
- Wenn Sie Service Accounts für Aufgaben nach der Installation verwenden.

9.4.1 Erstellen eines Konfigurationspakets für SafeGuard Enterprise Client (managed)

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**.
2. Wählen Sie **Konfigurationspaket (managed)** erstellen.
3. Klicken Sie auf **Konfigurationspaket hinzufügen**.
4. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
5. Ordnen Sie einen primären SafeGuard Enterprise Server zu (der sekundäre Server ist nicht zwingend notwendig).

6. Falls erforderlich, geben Sie eine Richtliniengruppe an, die auf die Computer angewendet werden soll. Diese müssen Sie zuvor im SafeGuard Management Center erstellt haben. Wenn Sie für Aufgaben nach der Installation auf dem Computer Service Accounts verwenden möchten, stellen Sie sicher, dass die entsprechende Richtlinieneinstellung in dieser ersten Richtliniengruppe definiert ist, *siehe Service Accounts für die Durchführung von Aufgaben nach der Installation* (Seite 61).
7. Wählen Sie den Modus für die **Transportverschlüsselung**, der bestimmt, wie die Verbindung zwischen SafeGuard Enterprise Client und SafeGuard Enterprise Server verschlüsselt wird: SafeGuard-Verschlüsselung oder SSL-Verschlüsselung.

   Der Vorteil bei SSL ist, dass es ein Standardprotokoll ist und eine schnellere Verbindung aufgebaut werden kann als mit der SafeGuard Transportverschlüsselung. Für weitere Informationen, *siehe Einrichten von SSL* (Seite 9).
8. Geben Sie einen Ausgabepfad für das Konfigurationspaket (MSI) an.
9. Klicken Sie auf **Konfigurationspaket erstellen**.

Das Konfigurationspaket (MSI) wird im angegebenen Verzeichnis angelegt. Im nächsten Schritt verteilen Sie das Paket an die SafeGuard Enterprise Client (managed) Endpoint-Computer zur Installation.

9.4.2 Erstellen eines Konfigurationspakets für Sophos SafeGuard (standalone)

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**.
2. Wählen Sie **Konfigurationspaket (standalone) erstellen**.
3. Klicken Sie auf **Konfigurationspaket hinzufügen**.
4. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
5. Geben Sie eine zuvor im SafeGuard Management Center erstellte **Richtliniengruppe** an, die für die Computer gelten soll.
6. Geben Sie unter **Speicherort für Schlüssel-Sicherungskopie** einen freigegebenen Netzwerkpfad für das Speichern der Schlüssel-Recovery-Datei an oder wählen Sie einen Netzwerkpfad aus. Geben Sie den freigegebenen Pfad in folgender Form ein: **\\networkcomputer**, z. B. **\\mycompany.edu**. Wenn Sie hier keinen Pfad angeben, wird der Benutzer beim ersten Anmelden am Endpoint-Computer nach der Installation gefragt, wo die Schlüsseldatei gespeichert werden soll.

   Die Schlüssel-Recovery-Datei (XML) wird für die Durchführung von Recovery-Vorgängen bei durch Sophos SafeGuard geschützten Computern benötigt. Sie wird auf allen durch Sophos SafeGuard geschützten Computern erzeugt.

   Hinweis:

   Stellen Sie sicher, dass diese Schlüssel-Recovery-Datei an einem Speicherort abgelegt wird, auf den die Mitarbeiter des Helpdesk Zugriff haben. Die Dateien können dem Helpdesk auch über andere Mechanismen zur Verfügung gestellt werden. Die Datei ist mit dem Unternehmenszertifikat verschlüsselt. Sie kann also auch auf externen Medien oder auf dem Netzwerk gespeichert werden, um sie dem Helpdesk für Recovery-Vorgänge zur Verfügung zu stellen. Sie kann auch per E-Mail verschickt werden.

7. Unter **POA Gruppe** können Sie eine POA Access Account Gruppe auswählen, die dem Endpoint-Computer zugeordnet wird. POA Access Accounts bieten Zugang für administrative Aufgaben auf dem Endpoint-Computer, nachdem die Power-on Authentication aktiviert wurde. Um POA Access Accounts zuzuweisen, müssen Sie die POA-Gruppe zunächst im Bereich **Benutzer und Computer** des SafeGuard Management Center anlegen.
8. Geben Sie einen Ausgabepfad für das Konfigurationspaket (MSI) an.
9. Klicken Sie auf **Konfigurationspaket erstellen**.

Das Konfigurationspaket (MSI) wird im angegebenen Verzeichnis angelegt. Im nächsten Schritt verteilen Sie das Paket an die Endpoint-Computer zur Installation.

9.4.3 Service Accounts für die Durchführung von Aufgaben nach der Installation

Wenn Sie SafeGuard Enterprise über einen zentralen Rollout-Vorgang installieren möchten, empfehlen wir die Konfiguration einer Service Account-Liste. Ein IT-Administrator, der zu einer Service Account-Liste hinzugefügt wurde, kann sich nach der Installation von SafeGuard Enterprise an Computern anmelden, ohne die Power-on Authentication zu aktivieren. Ein solches Vorgehen ist empfehlenswert, da normalerweise der erste Benutzer, der sich nach der Installation an einem Endpoint-Computer anmeldet, als primäres Benutzerkonto zur POA hinzugefügt wird. Die in den Listen enthaltenen Benutzer werden als SafeGuard Enterprise Gastbenutzer behandelt.

Mit Service Accounts ergibt sich folgender Workflow:

- SafeGuard Enterprise wird auf einem Endpoint-Computer installiert.
- Der Computer wird neu gestartet und ein Rollout-Beauftragter, der in einer Service Account Liste aufgeführt ist, meldet sich über die Windows-Eingabe-Aufforderung an.
- Gemäß der auf den Computer angewendeten Service Account Liste wird der Benutzer als Service Account erkannt und als Gastbenutzer behandelt.
- Der Rollout-Beauftragte wird nicht zur POA hinzugefügt und die POA wird nicht aktiviert. Der Endbenutzer kann sich anmelden und die POA aktivieren.

Hinweis:

Service Account Listen müssen Sie in einer Richtlinie anlegen und diese der ersten Richtliniengruppe des ersten Konfigurationspakets zuweisen, das Sie nach der Installation der Verschlüsselungssoftware auf dem Endpoint-Computer installieren. Weitere Informationen finden Sie in der Administrator-Hilfe.

10 Zentrales Einrichten von Endpoint-Computern

Durch das zentrale Einrichten von Endpoint-Computern wird eine standardisierte Installation auf mehreren Computern erreicht.

Die Installation und Konfiguration wird sowohl für SafeGuard Enterprise Clients (managed) als auch für Sophos SafeGuard Clients (standalone) beschrieben. Die Installationsschritte sind identisch, mit der Ausnahme, dass für jeden der beiden ein unterschiedliches Konfigurationspaket zugeordnet werden muss.

Die erforderlichen Arbeitsschritte werden auch für Endpoint-Computer mit Windows BitLocker Device Encryption beschrieben. Für Informationen zum Vorbereiten der BitLocker-Unterstützung, *siehe Spezifische vorbereitende Maßnahmen für die Unterstützung von BitLocker Device Encryption* (Seite 58).

Das Verhalten des Endpoint-Computers bei der ersten Anmeldung nach der Installation von SafeGuard Enterprise ist in der Benutzerhilfe beschrieben.

Hinweis:

Die Installations- und Konfigurationspakete dürfen im Rahmen einer zentralen Softwareverteilung nur einem Computer zugewiesen werden, nicht aber einem Benutzer.

10.1 Zentrales Installieren der Verschlüsselungssoftware

1. Bereiten Sie die Installation auf den Endpoint-Computern vor, *siehe Vorbereiten der Verschlüsselung* (Seite 57).

2. Verwenden Sie Ihre eigenen Tools, um das Installationspaket zu erstellen, das auf den Endpoint-Computern installiert werden soll. Das Paket muss Folgendes in der angegebenen Reihenfolge enthalten:

Element	Beschreibung
Vorbereitendes Installationspaket SGxClientPreinstall.msi	Das Paket stattet die Endpoint-Computer mit den nötigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware aus, zum Beispiel mit der benötigten DLL **MSVCR80.dll**, Version 8.0.50727.4053. **Hinweis:** Wenn dieses Paket nicht installiert ist, wird die Installation der Verschlüsselungssoftware abgebrochen.
Verschlüsselungssoftware-Installationspaket	Für die für SafeGuard Enterprise Clients (managed) verfügbaren Pakete, *siehe Installationspakete für SafeGuard Enterprise Clients (managed)* (Seite 53). Für die für Sophos SafeGuard Clients (standalone) verfügbaren Pakete, *siehe Installationspakete für Sophos SafeGuard Clients (standalone)* (Seite 54).
Konfigurationspaket für Endpoint-Computer	Verwenden Sie die zuvor im SafeGuard Management Center erzeugten Konfigurationspakete. Für SafeGuard Enterprise Clients (managed) und Sophos SafeGuard Clients (standalone) müssen unterschiedliche Konfigurationspakete erstellt werden, *siehe Erstellen von Konfigurationspaketen - Überblick* (Seite 59). Bevor Sie ein neues Konfigurationspaket installieren, deinstallieren sie zunächst veraltete Konfigurationspakete.
Skript mit Befehlen für die automatische Installation	Wir empfehlen, das Windows Installer Kommandozeilen-Tool **msiexec.exe** zu verwenden, um das Skript zu erzeugen. Für weitere Informationen *siehe Kommando für zentrale Installation* (Seite 64) oder *http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx*.

3. Erstellen Sie ein Verzeichnis mit der Bezeichnung **Software** als zentralen Speicherort für alle Anwendungen.
4. Um das Skript zu erzeugen, öffnen Sie eine Befehlseingabeaufforderung und geben Sie die Scripting-Befehle ein.
5. Verteilen Sie das Paket über unternehmensinterne Software-Verteilungsmechanismen an die Endpoint-Computer.

   Das Paket wird auf den Endpoint-Computern ausgeführt. Danach sind die Endpoint-Computer für den Einsatz von SafeGuard Enterprise bereit.

6. Starten Sie nach der Installation die Endpoint-Computer zweimal neu, um die Power-on Authentication zu aktivieren. Starten Sie den Computer ein drittes Mal neu, um eine Sicherung der Kerneldaten bei jedem Windows-Start durchzuführen. Diese Sicherungskopie wird nicht erstellt, wenn der Endpoint-Computer nur in den Ruhezustand oder in den Standby-Modus versetzt wird. Stellen Sie sicher, dass der Computer nicht in den Ruhezustand oder den Standby-Modus versetzt sondern ein drittes Mal neu gestartet wird, um eine Sicherung des Kernel zu erstellen.

Zusätzliche Konfiguration kann erforderlich sein, damit sich die Power-on Authentication (POA) auf jeder Hardware-Plattform korrekt verhält. Die meisten Hardware-Konflikte lassen sich mit Hilfe von **Hotkeys**-Funktionalitäten beheben, die in die POA integriert sind. Hotkeys können nach der Installation konfiguriert werden, entweder in der POA selbst oder über eine zusätzliche Konfigurationseinstellung, die dem Windows Installer Befehl msiexec mitgegeben wird. Weitere Informationen finden Sie hier:

http://www.sophos.de/support/knowledgebase/article/107781.html

http://www.sophos.de/support/knowledgebase/article/107785.html

10.2 Kommando für zentrale Installation

Verwenden Sie zur zentralen Installation von SafeGuard Enterprise auf den Endpoint-Computern die Windows Installer Komponente **msiexec**. **Msiexec** ist in Windows XP, Vista und Windows 7 bereits integriert und führt eine vorgefertigte SafeGuard Enterprise Installation automatisch aus. Sie können auch eine Quelle und ein Ziel für die Installation angeben. Eine Standardinstallation auf mehreren Endpoint-Computern steht zur Verfügung.

Weitere Informationen finden Sie hier:
http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx.

Kommandozeilen-Syntax

```
msiexec /i <path+msi package name> /qn ADDLOCAL=ALL | <SGN
Features> <SGN parameter>
```

Die Kommandozeilensyntax setzt sich folgendermaßen zusammen:

- Windows Installer Parameter, die z. B. Warnungen und Fehlermeldungen während der Installation in eine Datei protokollieren.
- Sophos SafeGuard Features, die installiert werden sollen, z. B. volume-basierende Verschlüsselung.
- Sophos SafeGuard Parameter, die z. B. das Installationsverzeichnis angeben.

Kommandooptionen

Alle verfügbaren Optionen können Sie über msiexec.exe in der Eingabeaufforderung abrufen. Im Folgenden sind wichtige Optionen beschrieben.

Option	Beschreibung
/i	Gibt an, dass es sich um eine Installation handelt.
/qn	Installiert ohne Benutzerinteraktion und zeigt keine Benutzeroberfläche an.
ADDLOCAL=	Listet die Features auf, die installiert werden. Wird die Option nicht angegeben, werden alle Features installiert, die für eine Standardinstallation vorgesehen sind. Beachten Sie: Trennen Sie die Features durch Kommas, nicht durch Leerzeichen. Achten Sie außerdem auf die Groß-/Kleinschreibung. Fügen Sie alle übergeordneten Features (Feature Parents) für das ausgewählte Feature zur Kommandozeile hinzu.
ADDLOCAL=ALL	Installiert alle verfügbaren Features.
REBOOT=Force | ReallySuppress	Erzwingt oder unterdrückt einen Neustart nach der Installation. Ohne Angabe wird der Neustart erzwungen (Force).
/L* <path + filename>	Protokolliert alle Warnungen und Fehlermeldungen in die angegebene Protokolldatei. Der Parameter **/Le <path + filename>** protokolliert ausschließlich Fehlermeldungen.
Installdir= <Verzeichnis>	Gibt das Verzeichnis an, in das der SafeGuard Enterprise Client installiert wird. Ohne Angabe wird als Standardinstallationsverzeichnis <SYSTEM>:\PROGRAMME\SOPHOS verwendet.

10.3 SafeGuard Enterprise Features (ADDLOCAL)

Für eine zentrale Installation müssen Sie bereits im Vorfeld definieren, welche Sophos SafeGuard Features auf den Endpoint-Computern installiert werden sollen. Listen Sie die Features nach der Eingabe der Option **ADDLOCAL** auf.

Hinweis:

Es ist zwar möglich, bei einer Erstinstallation nicht alle Features zu installieren, wir empfehlen jedoch, das Feature Device Encryption (volume-basierende Verschlüsselung) von Beginn an zu installieren.

Entscheiden Sie vor der Installation, ob Sie SafeGuard Enterprise in Verbindung mit der BitLocker Drive Encryption oder nur die native SafeGuard Enterprise Verschlüsselung anwenden möchten.

In den folgenden Tabellen sind alle SafeGuard Enterprise Features aufgelistet, die auf den Endpoint-Computern installiert werden können. Weitere Informationen finden Sie hier: *http://www.sophos.de/support/knowledgebase/article/108426.html*.

10.3.1 Features für SafeGuard Device Encryption

Hinweis:

Die Features **Client** und **Authentication** müssen Sie standardmäßig auflisten. Wenn Sie ein Feature auswählen, müssen Sie auch alle übergeordneten Features (Feature Parents) zur Kommandozeile hinzufügen!

Feature Parents	Feature
Client	**Authentication** Das Feature **Authentication** und sein Feature Parent **Client** müssen standardmäßig angegeben werden.
Client, Authentication	**CredentialProvider** Für Computer mit Windows Vista und Windows 7 müssen Sie dieses Feature installieren. Es dient zur Anmeldung über den Credential Provider.
Client, BaseEncryption	**SectorBasedEncryption** Installiert die volume-basierende Verschlüsselung von SafeGuard Enterprise mit den folgenden Funktionen: Alle Volumes, auch Wechselmedien, lassen sich mit der volume-basierenden Verschlüsselung von SafeGuard Enterprise verschlüsseln. Sophos SafeGuard Power-on Authentication (POA) Sophos SafeGuard Recovery mit Challenge/Response **Hinweis:** Es kann entweder SectorBasedEncryption ODER BitLockerSupport angegeben werden.
Client	**SecureDataExchange** SafeGuard Data Exchange mit dateibasierender Verschlüsselung wird immer auf lokaler Ebene und für Wechselmedien installiert. SafeGuard Data Exchange sorgt für die sichere Verschlüsselung von Wechselmedien. Daten können sicher und einfach mit anderen Benutzern ausgetauscht werden. Alle Ver- und Entschlüsselungsvorgänge laufen transparent und mit minimaler Benutzerinteraktion ab. Wenn Sie SafeGuard Data Exchange auf Ihrem Computer installiert haben, wird auch SafeGuard Portable installiert. SafeGuard Portable ermöglicht den sicheren Datenaustausch mit Computern, auf denen SafeGuard Data Exchange nicht installiert ist. **Hinweis:**

Feature Parents	Feature
	SafeGuard Data Exchange kann parallel zum BitLocker Client installiert werden.
Client	**BitLockerSupport** Installiert die BitLocker-Unterstützung für SafeGuard Enterprise mit den folgenden Funktionen: Boot-Volume-Verschlüsselung mit BitLocker Verschlüsselung weiterer Volumes mit BitLocker BitLocker Pre-Boot Authentication BitLocker Recovery Es kann entweder **SectorBasedEncryption** ODER **BitLockerSupport** angegeben werden. **Hinweis:** Für Sophos SafeGuard Clients (standalone) nicht verfügbar.
Client	**ConfigurationProtection** Schnittstellenschutz und Management von Peripheriegeräten: Um SafeGuard Configuration Protection zu installieren, müssen Sie das Feature im **msiexec** Kommando des Client-Installationspakets angeben UND zusätzliche Installationsschritte durchführen, *siehe Einrichten von SafeGuard Configuration Protection* (Seite 78). **Hinweis:** Für Sophos SafeGuard Clients (standalone) nicht verfügbar.

10.3.2 Features für SafeGuard Data Exchange

Hinweis:

Die Features **Client** und **Authentication** müssen Sie standardmäßig auflisten. Wenn Sie ein Feature auswählen, müssen Sie auch alle übergeordneten Features (Feature Parents) zur Kommandozeile hinzufügen!

Feature Parents	Feature
Client	**Authentication** Das Feature **Authentication** und sein Feature Parent **Client** müssen standardmäßig angegeben werden.
Client	**SecureDataExchange**

Feature Parents	Feature
	SafeGuard Data Exchange mit dateibasierender Verschlüsselung wird immer auf lokaler Ebene und für Wechselmedien installiert. SafeGuard Data Exchange sorgt für die sichere Verschlüsselung von Wechselmedien. Daten können sicher und einfach mit anderen Benutzern ausgetauscht werden. Alle Ver- und Entschlüsselungsvorgänge laufen transparent und mit minimaler Benutzerinteraktion ab. Wenn Sie SafeGuard Data Exchange auf Ihrem Computer installiert haben, ist auch SafeGuard Portable installiert. SafeGuard Portable ermöglicht den sicheren Datenaustausch mit Computern, auf denen SafeGuard Data Exchange nicht installiert ist.
Client	**ConfigurationProtection** Schnittstellenschutz und Management von Peripheriegeräten: Um SafeGuard Configuration Protection zu installieren, müssen Sie das Feature im **msiexec**-Kommando des Client-Installationspakets angeben UND zusätzliche Installationsschritte durchführen, *siehe Einrichten von SafeGuard Configuration Protection* (Seite 78). **Hinweis:** Für Sophos SafeGuard Clients (standalone) nicht verfügbar.

10.3.3 Beispielkommando für volume- und dateibasierende Verschlüsselung

Folgendes wird durch das unten aufgeführte Kommando ausgeführt:

- Die Endpoint-Computer werden mit den notwendigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware ausgestattet.
- SafeGuard Enterprise Power-on Authentication wird installiert.
- SafeGuard Enterprise volume-basierende Verschlüsselung wird installiert.
- SafeGuard Data Exchange für dateibasierende Verschlüsselung wird über die Angabe von **SecureDataExchange** installiert.
- Es wird eine Protokolldatei angelegt.
- Das Konfigurationspaket für den SafeGuard Enterprise Client (managed) wird ausgeführt.

Beispiel:

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log
I:\Temp\SGNClient.log
```

```
ADDLOCAL=Client,Authentication,BaseEncryption,SectorBasedEncryption,
 SecureDataExchange
```

```
Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGNConfig.msi /qn /log
I:\Temp\SGNConfig.log
```

10.3.4 Beispielkommando für BitLocker-Unterstützung unter Windows Vista

Folgendes wird durch das unten aufgeführte Kommando ausgeführt:

- Die Endpoint-Computer werden mit den notwendigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware ausgestattet.
- Benutzer melden sich an ihren Computern über den Windows Vista Credential Provider an.
- SafeGuard Enterprise BitLocker-Unterstützung mit BitLocker volume-basierender Verschlüsselung wird installiert.
- SafeGuard Data Exchange für dateibasierende Verschlüsselung wird über die Angabe von **SecureDataExchange** installiert.
- Es wird eine Protokolldatei angelegt.
- Anschließend wird das Konfigurationspaket für den SafeGuard Enterprise Client (managed) ausgeführt.

Hinweis:

Stellen Sie für die Installation von SafeGuard Enterprise mit BitLocker sicher, dass nur **BitLockerSupport** ausgeführt wird. Nehmen Sie SafeGuard Enterprise **BaseEncryption** nicht in die Kommandozeile auf.

Beispiel:

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log
I:\Temp\SGNClient.log
```

```
ADDLOCAL=Client,Authentication,CredentialProvider,
BaseEncryption,BitLockerSupport, SecureDataExchange
```

```
Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGNConfig.msi /qn /log
I:\Temp\SGNConfig.log
```

10.4 Installation gemäß FIPS

Die FIPS-Zertifizierung beschreibt Sicherheitsanforderungen für Verschlüsselungsmodule. So stellen z. B. Behörden in den USA und in Kanada an Software für besonders sicherheitskritische Informationen die Anforderung der FIPS 140-2 Zertifizierung.

SafeGuard Enterprise nutzt FIPS-zertifizierte AES-Algorithmen. Standardmäßig wird eine neue, schnellere Implementierung der AES-Algorithmen installiert, die noch nicht FIPS-zertifiziert ist.

Um die FIPS-zertifizierte Variante des AES-Algorithmus zu nutzen, setzen Sie beim Installieren der SafeGuard Enterprise Verschlüsselungssoftware die Eigenschaft FIPS_AES auf 1.

Hierzu gibt es zwei Möglichkeiten:

- Fügen Sie die Eigenschaft zum Kommandozeilen-Skript hinzu:
  msiexec /i F:\Software\SGNClient.msi FIPS_AES=1
- Verwenden Sie ein Transform.

10.5 Installation auf Endpoint-Computern mit selbst-verschlüsselnden Opal-Festplatten

SafeGuard Enterprise unterstützt den anbieter-unabhängigen Opal-Standard für selbst-verschlüsselnde Festplatten und bietet die Verwaltung von Endpoint-Computern mit dieser Art von Festplatten.

Um sicherzustellen, dass die Unterstützung von selbst-verschlüsselnden Opal-Festplatten diesem Standard möglichst genau entspricht, werden bei der Installation von SafeGuard Enterprise auf dem Endpoint-Computer zwei Arten von Prüfungen durchgeführt:

- **Funktionale Prüfungen**

  Hier wird u. a. geprüft, ob sich die Festplatte als "OPAL"-Festplatte identifiziert, ob Kommunikationseinstellungen korrekt sind und ob alle für SafeGuard Enterprise erforderlichen Opal Features von der Festplatte unterstützt werden.

- **Sicherheitsprüfungen**

  Mit Sicherheitsprüfungen wird sichergestellt, dass nur SafeGuard Enterprise Benutzer auf der Festplatte registriert sind und dass nur SafeGuard Enterprise Benutzer die Schlüssel für die software-basierende Verschlüsselung von nicht selbst-verschlüsselnden Laufwerken haben. Wird bei der Installation festgestellt, dass andere Benutzer registriert sind, versucht SafeGuard Enterprise automatisch, diese zu deaktivieren. Diese Funktionalität wird durch den Opal-Standard gefordert. Ausgenommen sind hier einige wenige Standard "Authorities", die für den Betrieb eines Opal-Systems erforderlich sind.

Hinweis:

Diese Sicherheitsprüfungen werden wiederholt, wenn nach einer erfolgreichen Installation im Opal-Modus eine Verschlüsselungsrichtlinie für die Festplatte angewendet wird. Schlagen die Sicherheitsprüfungen in diesem Fall fehl, so haben inzwischen außerhalb von SafeGuard Enterprise Eingriffe in die Laufwerksverwaltung stattgefunden. In diesem Fall verweigert SafeGuard Enterprise den Zugriff auf das Laufwerk und es wird eine entsprechende Meldung angezeigt.

Sollten einige dieser Prüfungen ohne Recovery-Möglichkeit fehlschlagen, so wird für die Installation nicht die software-basierende Verschlüsselung angewendet. Stattdessen bleiben alle Volumes auf der Opal-Festplatte unverschlüsselt.

Bei einigen Opal-Festplatten bestehen u. U. Sicherheitsprobleme. Es besteht keine Möglichkeit, automatisch festzustellen, welche Privilegien unbekannten Benutzern/Authorities zugeordnet sind, die bereits zum Zeitpunkt der SafeGuard Enterprise Installation/Verschlüsselung registriert waren. Wenn die Festplatte den Befehl, diese Benutzer zu deaktivieren, nicht ausführt, wendet SafeGuard Enterprise die software-basierende Verschlüsselung an, um die größtmögliche Sicherheit für den SafeGuard Enterprise Benutzer zu gewährleisten. Da wir für die Festplatten selbst keine Sicherheitsgarantien geben können, haben wir einen speziellen Installationsschalter implementiert. Diesen Schalter können Sie verwenden, um Festplatten mit potentiellen Sicherheitsrisiken auf eigene Verwantwortung zu benutzen. Eine Liste der Festplatten, für die dieser Schalter erforderlich ist, sowie weitere Informationen zu unterstützten Festplatten finden Sie in den SafeGuard Enterprise Release Notes.

Um den Installationsschalter anzuwenden, benutzen Sie folgende Kommandozeilensyntax:

```
MSIEXEC /i <Name_des_ausgewählten_Client_MSI.msi>
IGNORE_OPAL_AUTHORITYCHECK_RESULTS=1
```

Die interne Eigenschaft des .msi-Pakets hat denselben Namen. Diese Information benötigen Sie, wenn Sie z. B. eine Installation mit .mst-Dateien ausführen oder Ihre .msi-Datei z. B. mit ORCA modifizieren möchten.

Weitere Informationen zu SafeGuard Enterprise in Kombination mit Opal-Festplatten finden Sie in der SafeGuard Enterprise Administratorhilfe und Benutzerhilfe.

11 Lokales Einrichten von Endpoint-Computern

Wenn Sie erst eine Probeinstallation auf einem Endpoint-Computer durchführen möchten, ist es sinnvoll, SafeGuard Enterprise zunächst lokal zu installieren.

Die Installation und Konfiguration wird sowohl für SafeGuard Enterprise Clients (managed) als auch für Sophos SafeGuard Clients (standalone) beschrieben. Die Installationsschritte sind identisch, mit der Ausnahme, dass für jeden der beiden ein unterschiedliches Konfigurationspaket zugeordnet werden muss.

Die erforderlichen Arbeitsschritte werden auch für Endpoint-Computer mit Windows BitLocker Device Encryption beschrieben. Für Informationen zum Vorbereiten der BitLocker-Unterstützung, *siehe Spezifische vorbereitende Maßnahmen für die Unterstützung von BitLocker Device Encryption* (Seite 58).

Das Verhalten des Endpoint-Computers bei der ersten Anmeldung nach der Installation von SafeGuard Enterprise ist in der Benutzerhilfe beschrieben.

11.1 Lokales Installieren der Verschlüsselungssoftware

So führen Sie eine lokale Installation der Verschlüsselungssoftware durch:

1. Bereiten Sie die Installation auf den Endpoint-Computern vor, *siehe Vorbereiten der Verschlüsselung* (Seite 57).
2. Melden Sie sich an dem Computer als Administrator an.
3. Installieren Sie das Prä-Installationspaket **SGxClientPreinstall.msi**, das den Endpoint-Computer mit den nötigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware ausstattet.

   Hinweis: Alternativ können Sie auch die Datei **vcredist_x86.exe** installieren, die Sie hier herunterladen können: *http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2*, oder sicherstellen, dass sich die DLL **MSVCR80.dll** in der Version 8.0.50727.4053 im Verzeichnis Windows\WinSxS auf dem Computer befindet.

4. Klicken Sie auf dem relevanten <Client> Installationspaket (MSI) doppelt, um den Installationsassistenten der Verschlüsselungssoftware zu starten. Dieser führt Sie durch die notwendigen Schritte.
5. Übernehmen Sie in den folgenden Dialogen die Standardeinstellungen.
6. Wählen Sie ggf. den Installationstyp und die Features gemäß Ihren Anforderungen aus. Kunden, die SGNClient.msi oder SGNClient_x64.msi installieren, führen einen der folgenden Handlungsschritte aus:

   - Wählen Sie **Vollständig**, um sowohl SafeGuard Enterprise Device Protection als auch Data Exchange zu installieren.
   - Wählen Sie **Typisch**, um nur SafeGuard Enterprise Device Protection zu installieren.
   - Wählen Sie **Angepasst**, um sowohl BitLocker Device Encryption zu installieren. Wählen Sie unter **Features** das Feature **Device Encryption**, aktivieren Sie **BitLocker Support** und deaktivieren Sie **Base Encryption**.

   Hinweis:

Es ist zwar möglich, bei einer Erstinstallation nicht alle Features zu installieren, wir empfehlen jedoch, das Feature Device Encryption (volume-basierende Verschlüsselung) von Beginn an zu installieren.

7. Übernehmen Sie in allen weiteren Dialogen die Standardeinstellungen, um den Installationsassistenten abzuschließen.

   SafeGuard Enterprise wird auf dem Endpoint-Computer installiert.

8. Wechseln Sie an den Speicherort des Standard-Konfigurationspakets (MSI), das Sie zuvor im SafeGuard Management Center erzeugt haben. Für SafeGuard Enterprise Clients (managed) und Sophos SafeGuard Clients (standalone) müssen unterschiedliche Konfigurationspakete erstellt werden, *siehe Erstellen von Konfigurationspaketen - Überblick* (Seite 59).
9. Installieren Sie das relevante Konfigurationspaket (MSI) auf dem Computer.

SafeGuard Enterprise wird auf dem Endpoint-Computer eingerichtet. Melden Sie sich nun zum ersten Mal nach der Installation an dem Computer an. Informationen zum Verhalten des Computers nach der Installation von SafeGuard Enterprise finden Sie in der Benutzerhilfe.

12 Installieren von SafeGuard Enterprise auf einem Computer mit mehreren Betriebssystemen

Die SafeGuard Enterprise Verschlüsselungssoftware kann auch dann auf einem Computer zum Schutz der Daten installiert werden, wenn mehrere Betriebssysteme auf separaten Volumes der Festplatte installiert sind. SafeGuard Enterprise bietet ein so genanntes Runtime-System. SafeGuard Enterprise Runtime stellt folgende Sachverhalte sicher, wenn die Software auf Volumes mit einer zusätzlichen Windows-Installation installiert wird:

- Die Windows-Installation, die sich auf diesen Volumes befindet, kann erfolgreich durch einen Boot Manager gestartet werden.
- Auf Partitionen auf diesen Volumes, die durch eine vollständige SafeGuard Enterprise Client Installation mit dem definierten Computerschlüssel verschlüsselt worden sind, kann erfolgreich zugegriffen werden.

12.1 Voraussetzungen und Einschränkungen

Beachten Sie:

- SafeGuard Enterprise Runtime bietet keine SafeGuard Enterprise Client spezifischen Features oder Funktionalitäten.
- SafeGuard Enterprise Runtime unterstützt nur die Betriebssysteme, die auch für die SafeGuard Enterprise Verschlüsselungssoftware unterstützt werden.
- USB-Tastaturen können u. U. nur eingeschränkt benutzt werden.
- Es werden nur Boot Manager unterstützt, die nach der Power-on Authentication aktiv werden.
- Die Unterstützung von Boot Managern von Drittanbietern wird nicht garantiert. Wir empfehlen den Einsatz von Microsoft Boot Managern.
- SafeGuard Enterprise Runtime kann nicht auf eine SafeGuard Enterprise Client Installation in Vollversion aktualisiert werden.
- Das Runtime-Installationspaket muss vor der Vollversion des Enterprise Client Pakets installiert werden.
- Es kann nur auf Volumes, die mit dem definierten Computerschlüssel in SafeGuard Enterprise verschlüsselt wurden, zugegriffen werden.

12.2 Vorbereitung

Um SafeGuard Enterprise Runtime einzurichten, führen Sie die folgenden vorbereitenden Schritte in der angegebenen Reihenfolge durch:

1. Stellen Sie sicher, dass die Volumes, auf denen SafeGuard Enterprise Runtime laufen soll, zum Zeitpunkt der Installation sichtbar sind und mit ihrem Windows-Namen (z. B. C:) angesprochen werden können.

2. Legen Sie fest, auf welchem Volume/welchen Volumes der Festplatte SafeGuard Enterprise Runtime installiert werden soll. In Zusammenhang mit SafeGuard Enterprise sind diese Volumes als "sekundäre" Windows-Installationen definiert. Es können mehrere sekundäre Windows-Installationen vorhanden sein. Verwenden Sie folgendes Paket: SGNClientRuntime.msi oder SGNClientRuntime_x64.msi (unter Windows Vista 64 Bit, Window 7 64 Bit).
3. Legen Sie fest, auf welchem Volume der Festplatte die Vollversion des SafeGuard Enterprise Clients installiert werden soll. In Zusammenhang mit SafeGuard Enterprise ist dieses Volume als “primäre“ Windows-Installation definiert. Es kann jeweils nur eine primäre Windows-Installation geben. Verwenden Sie folgendes Paket: SGNClient.msi oder SGNClient_x64.msi (unter Windows Vista 64 Bit, Window 7 64 Bit). Falls erforderlich können Sie zusätzlich Configuration Protection (SGN_CP_Client.msi / SGN_CP_Client_x64.msi verfügbar für Windows 7 64-Bit-Betriebssysteme) installieren.

12.3 Einrichten von SafeGuard Enterprise Runtime

1. Wählen Sie das/die gewünschte(n) sekundäre(n) Volume(s) der Festplatte aus, auf dem/denen Sie SafeGuard Enterprise Runtime Client installieren möchten.
2. Starten Sie die sekundäre Windows-Installation auf dem ausgewählten Volume.
3. Installieren Sie das Runtime-Installationspaket auf dem ausgewählten Volume.
4. Übernehmen Sie die Standardeinstellungen im nächsten Dialog des Installers. Sie müssen keine speziellen Features auswählen.
5. Wählen Sie einen Installationsordner für die Runtime-Installation.
6. Klicken Sie auf **Beenden**, um die Runtime-Installation abzuschließen.
7. Wählen Sie das primäre Volume der Festplatte, auf dem Sie SafeGuard Enterprise Client installieren möchten.
8. Starten Sie die primäre Windows-Installation auf dem ausgewählten Volume.
9. Starten Sie das vorbereitende Installationspaket SGxClientPreinstall.msi. Dieses Paket stattet die Endpoint-Computer mit notwendigen Voraussetzungen für die erfolgreiche Installation der Verschlüsselungssoftware aus.
10. Installieren Sie das SafeGuard Enterprise Client Installationspaket auf dem ausgewählten Volume.
11. Erstellen Sie ein Konfigurationspaket für einen SafeGuard Enterprise Client (managed) oder Sophos SafeGuard Client (standalone) je nach Anforderung und verteilen Sie diese an die Endpoint-Computer.
12. Verschlüsseln Sie beide Volumes mit dem definierten Computerschlüssel.

12.4 Starten von einem sekundären Volume über einen Boot Manager

1. Starten Sie den Computer.
2. Melden Sie sich an der Power-on Authentication mit Ihren Anmeldeinformationen an.
3. Starten Sie den Boot Manager und wählen Sie das gewünschte sekundäre Volume als Boot-Laufwerk.
4. Starten Sie den Computer von diesem Volume neu.

Auf jedes Volume, das mit dem definierten Computerschlüssel verschlüsselt ist, kann zugegriffen werden.

13 Einrichten von SafeGuard Configuration Protection

SafeGuard Configuration Protection ermöglicht es, nur bestimmte Schnittstellen und Peripheriegeräte auf den Endpoint-Computern zu erlauben. Dies verhindert, dass Malware auf den Endpoint-Computer gelangt, sowie Datenexporte über unerwünschte Kanäle, z. B. WLAN. SafeGuard Configuration Protection erkennt und blockiert auch gefährliche Hardware wie Key Logger.

13.1 Voraussetzungen und Einschränkungen

Beachten Sie folgende Voraussetzungen und Einschränkungen:

- Um SafeGuard Configuration Protection auf Windows 7 64-Bit-Betriebssystemen einzurichten, können Sie die 64-Bit-Varianten der "Client"-Installationspakete verwenden:
- Configuration Protection steht nur für SafeGuard Enterprise Clients (managed) zur Verfügung. SafeGuard Configuration Protection wird nicht für Sophos SafeGuard Clients (standalone) unterstützt.
- .NET Version 2.0 muss installiert sein.

13.2 Zentrales Installieren von SafeGuard Configuration Protection

Wenn Sie SafeGuard Configuration Protection zentral auf den Endpoint-Computern installieren möchten, verwenden Sie die Windows Installer-Komponente msiexec.

Die Kommandozeile lautet wie folgt:

```
msiexec /i SGN_CP_Client.msi /quiet /norestart
```

Um SafeGuard Configuration Protection zu installieren, führen Sie die folgenden Schritte in der angegebenen Reihenfolge durch:

1. Bereiten Sie die Installation auf den Endpoint-Computern vor, *siehe Vorbereiten der Verschlüsselung* (Seite 57).

2. Verwenden Sie Ihre eigenen Tools, um das Installationspaket zu erstellen, das auf den Endpoint-Computern installiert werden soll. Das Paket muss folgende Komponenten in der angegebenen Reihenfolge enthalten:

Vorbereitendes Installationspaket SGxClientPreinstall.msi	Das Paket stattet die Endpoint-Computer mit den nötigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware aus, zum Beispiel mit der benötigten DLL **MSVCR80.dll**, Version 8.0.50727.4053. **Hinweis:** Wenn dieses Paket nicht installiert ist, wird die Installation der Verschlüsselungssoftware abgebrochen.
SafeGuard Enterprise Verschlüsselungssoftware-Installationspaket.	Verwenden Sie entweder SafeGuard Device Encryption (SGNClient.msi) oder SafeGuard Data Exchange (SGN_withoutDe.msi). Um SafeGuard Configuration Protection auf Windows 7 64-Bit-Betriebssystemen einzurichten, können Sie die 64-Bit-Varianten der Client-Installationspakete verwenden. Fügen Sie ConfigurationProtection als Feature zur ADDLOCAL-Option hinzu.
SafeGuard Configuration Protection Installationspaket	Verwenden Sie SGN_CP_Client.msi. Um SafeGuard Configuration Protection auf Windows 7 64-Bit-Betriebssystemen einzurichten, können Sie die 64-Bit-Variante der Client-Installationspakete verwenden. Verwenden Sie den Parameter **/norestart**, um sicherzustellen, dass der Computer nicht neu gestartet wird: **msiexec /i SGN_CP_Client.msi /quiet /norestart**
Konfigurationspaket für den SafeGuard Enterprise Client (managed)	Verwenden Sie die zuvor im SafeGuard Management Center erzeugten Konfigurationspakete. Bevor Sie ein neues Konfigurationspaket installieren, deinstallieren sie zunächst vorhandene veraltete Konfigurationspakete.
Skript mit Befehlen für die automatische Installation	Wir empfehlen, das Windows Installer Kommandozeilen-Tool **msiexec.exe** zu verwenden, um das Skript zu erzeugen.

3. Erstellen Sie ein Verzeichnis mit der Bezeichnung **Software** als zentralen Speicherort für alle Anwendungen.
4. Um das Skript zu erzeugen, öffnen Sie eine Befehlseingabeaufforderung und geben Sie die Scripting-Befehle ein.
5. Verteilen Sie dieses Paket über unternehmenseigene Software-Verteilungsmechanismen an die Endpoint-Computer.

13.2.1 Beispielkommando für SafeGuard Configuration Protection mit SafeGuard Device Encryption

Das msiexec Kommando muss in der im Beispiel angegebenen Reihenfolge ausgeführt werden. In diesem Beispiel wird folgendes installiert:

- Die Endpoint-Computer werden mit den notwendigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware ausgestattet.
- SafeGuard Device Encryption mit volume-basierender Verschlüsselung wird installiert.
- SafeGuard Configuration Protection muss als Feature für das SafeGuard Device Encryption Installationspaket angegeben werden.
- Um die Installation des Moduls SafeGuard Configuration Protection anzustoßen, muss ein separates Installationspaket durch Angabe eines weiteren msiexec Kommandos hinzugefügt werden.
- Es wird eine Protokolldatei angelegt.
- Das Konfigurationspaket für den SafeGuard Enterprise Client (managed) wird ausgeführt.

Beispiel:

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn
/logI:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log
I:\Temp\SGNClient.log
ADDLOCAL=Client,Authentication,BaseEncryption,SectorBasedEncryption,ConfigurationProtection
```

```
Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGN_CP_Client.msi /quiet /norestart
```

```
msiexec /i F:\Software\SGNEnterpriseClientConfig.msi /qn /log
 I:\Temp\SGNEnterpriseClientConfig.log
```

13.2.2 Beispielkommando für SafeGuard Configuration Protection mit SafeGuard Data Exchange

Das msiexec Kommando muss in der im Beispiel angegebenen Reihenfolge ausgeführt werden. In diesem Beispiel wird folgendes installiert:

- Die Endpoint-Computer werden mit den notwendigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware ausgestattet.
- SafeGuard Data Exchange mit dateibasierender Verschlüsselung wird installiert.
- SafeGuard Configuration Protection muss als Feature für das SafeGuard Data Exchange Installationspaket angegeben werden.
- Um die Installation des Moduls SafeGuard Configuration Protection anzustoßen, muss ein separates Installationspaket durch Angabe eines weiteren msiexec Kommandos hinzugefügt werden.
- Es wird eine Protokolldatei angelegt.
- Das Konfigurationspaket für den SafeGuard Enterprise Client (managed) wird ausgeführt.

Beispiel:

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn
/logI:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log
I:\Temp\SGNClient.log
ADDLOCAL=Client,Authentication,SecureDataExchange,ConfigurationProtection
```

```
Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGN_CP_Client.msi /quiet /norestart
```

```
msiexec /i F:\Software\SGNEnterpriseClientConfig.msi /qn /log
 I:\Temp\SGNEnterpriseClientConfig.log
```

13.3 Lokales Installieren von SafeGuard Configuration Protection

Um SafeGuard Configuration Protection lokal zu installieren, führen Sie die folgenden Schritte in der angegebenen Reihenfolge durch:

1. Bereiten Sie die Installation auf den Endpoint-Computern vor, *siehe Vorbereiten der Verschlüsselung* (Seite 57).
2. Melden Sie sich an dem Computer als Administrator an.
3. Installieren Sie das vorbereitende MSI-Paket **SGxClientPreinstall.msi**, das den Endpoint-Computer mit den nötigen Voraussetzungen für eine erfolgreiche Installation der Verschlüsselungssoftware ausstattet.
4. Wählen Sie eines der folgenden SafeGuard Enterprise Client-Installationspakete für die Installation auf dem Endpoint-Computer. Um SafeGuard Configuration Protection auf Windows 7 64-Bit-Betriebssystemen einzurichten, können Sie die 64-Bit-Varianten der Client-Installationspakete verwenden:
   - SafeGuard Device Encryption (SGNClient.msi/SGNClient_x64.msi)
   - SafeGuard Data Exchange (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi.
5. Wählen Sie im Installationsassistenten den Installationstyp **Angepasst** aus. Wählen Sie unter **Features** zusätzlich das Feature **Configuration Protection**.
6. Installieren Sie das SafeGuard Configuration Protection Installationspaket SGN_CP_Client.msi/SGN_CP_Client_x64.msi (verfügbar für Windows 7 64-Bit-Betriebssysteme).

   Ändern Sie das Installationsverzeichnis in C:\Programme\Sophos\SafeGuard Enterprise\, um sicherzustellen, dass das Configuration Protection Module im SafeGuard Enterprise Verzeichnis installiert wird.
7. Starten Sie den Computer nicht neu.
8. Erzeugen Sie ein Konfigurationspaket für den SafeGuard Enterprise Client (managed) und installieren Sie es direkt nach der Installation der Verschlüsselungssoftware auf dem Endpoint-Computer.
9. Starten Sie den Endpoint-Computer neu.

SafeGuard Configuration Protection wird auf dem Endpoint-Computer installiert.

13.4 Deinstallieren von SafeGuard Configuration Protection

Um SafeGuard Configuration Protection zu deinstallieren, führen Sie die folgenden Schritte in der angegebenen Reihenfolge durch:

1. Deinstallieren Sie das SafeGuard Enterprise Client (managed) Konfigurationspaket.
2. Starten Sie das SafeGuard Enterprise Client Installationspaket auf dem Computer, entweder SGNClient.msi oder SGNClient_withoutDE.msi oder die entsprechende 64-Bit-Variante.
3. Wählen Sie im Installationsassistenten den Installationstyp **Angepasst** aus.
4. Deaktivieren Sie unter **Features** zusätzlich das Feature **Configuration Protection**.
5. Wenn die Deinstallation beendet ist, starten Sie den Computer auf keinen Fall neu.

6. Deinstallieren Sie das SafeGuard Configuration Protection Installationspaket SGN_CP_Client.msi/SGN_CP_Client_x64.msi.
7. Starten Sie den Computer neu.

SafeGuard Configuration Protection wird vom Endpoint-Computer entfernt.

13.5 Aktualisieren von SafeGuard Configuration Protection

Um SafeGuard Configuration Protection zu aktualisieren, führen Sie die folgenden Schritte in der angegebenen Reihenfolge durch:

1. Starten Sie das vorbereitende Installationspaket SGxClientPreinstall.msi. Dieses Paket stattet die Endpoint-Computer mit notwendigen Voraussetzungen für die erfolgreiche Installation der Verschlüsselungssoftware aus.
2. Starten Sie für die Aktualisierung das neueste SafeGuard Enterprise Client Installationspaket auf dem Computer, entweder SGNClient.msi oder SGNClient_withoutDE.msi oder die entsprechende 64-Bit-Variante. Um SafeGuard Configuration Protection auf Windows 7 64-Bit-Betriebssystemen einzurichten, können Sie die 64-Bit-Varianten der Client-Installationspakete verwenden.

   Starten Sie den Computer nach dem Abschluss der Aktualisierung nicht neu.
3. Entfernen Sie unter **Software** das SafeGuard SafeGuard Configuration Protection Client Installationspaket (SGN_CP_Client.msi).
4. Starten Sie den Endpoint-Computer neu.
5. Installieren Sie das neueste SafeGuard Configuration Protection Installationspaket SGN_CP_Client.msi/SGN_CP_Client_x64.msi.
6. Starten Sie den Endpoint-Computer neu.
7. Ordnen Sie im SafeGuard Management Center die relevante Configuration Protection Richtlinie dem Endpoint-Computer erneut zu, um die Funktion zu aktivieren.

SafeGuard Configuration Protection wird auf dem Endpoint-Computer aktualisiert.

14 Replikation der SafeGuard Enterprise Datenbank

Zur Optimierung der Performance lässt sich die SafeGuard Enterprise Datenbank auf mehrere SQL Server replizieren.

Dieses Kapitel beschreibt das Aufsetzen der Replikation für die SafeGuard Enterprise Datenbank in einer verteilten Umgebung. In der Beschreibung wird davon ausgegangen, dass Sie bereits Erfahrung mit dem Microsoft SQL Server Replikationsmechanismus haben.

Hinweis:

Die Administration sollte nur bei der Master-Datenbank erfolgen, nicht bei replizierten Datenbanken.

14.1 Mergereplikation

Die Mergereplikation ist der Vorgang der Verteilung von Daten vom Verleger an die Abonnenten. Dabei können Verleger und Abonnenten unabhängig voneinander Aktualisierungen vornehmen und danach einen Merge der Aktualisierungen zwischen den Standorten durchführen.

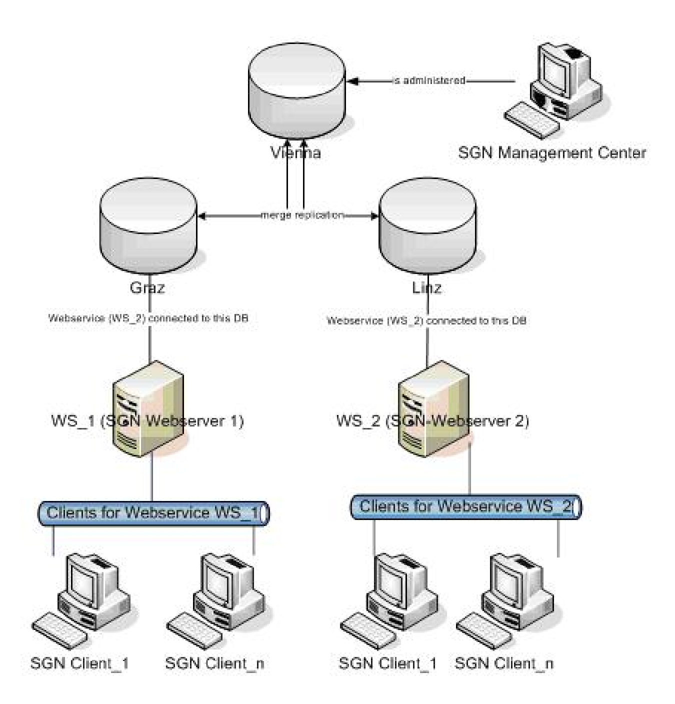
Die Mergereplikation erlaubt es verschiedenen Standorten, autonom zu arbeiten und später die Aktualisierungen zu einem einzigen, einheitlichen Ergebnis zusammenzuführen. Der initiale Snapshot wird auf die Abonnenten angewendet. Microsoft SQL Server verfolgt dann die Änderungen an veröffentlichten Daten beim Verleger und bei den Abonnenten nach. Die Daten werden zwischen den Servern kontinuierlich, zu einem festgelegten Zeitpunkt oder auf Anforderung synchronisiert. Da Aktualisierungen auf mehr als einem Server ausgeführt werden, sind dieselben Daten möglicherweise vom Verleger und von mindestens einem Abonnenten aktualisiert worden. Daher kann es beim Zusammenführen von Aktualisierungen zu Konflikten kommen.

Die Mergereplikation bietet Standardmöglichkeiten sowie individuelle Möglichkeiten für die Konfliktlösung, die Sie bei der Konfiguration einer Mergeveröffentlichung definieren können. Tritt ein Konflikt auf, ruft der Merge-Agent einen Resolver auf. Dieser bestimmt, welche Daten akzeptiert und an andere Standorte verteilt werden.

14.2 Einrichten der Datenbankreplikation

Der Vorgang des Einrichtens einer Replikation für die SafeGuard Enterprise Datenbank wird am Beispiel von Microsoft SQL Server 2005 beschrieben.

Im Beispiel wird SafeGuard Enterprise ausschließlich von der Datenbank in **Wien** aus administriert. Alle Änderungen werden vom SafeGuard Management Center über den Microsoft SQL Server 2005 Replikationsmechanismus an die Datenbanken in **Graz** und **Linz** weitergegeben. Die von den Client-Computern über die Web Server gemeldeten Änderungen werden ebenfalls über den Replikationsmechanismus an den Microsoft SQL Server 2005 weitergegeben.



14.2.1 Erzeugen der Master-Datenbank

Legen Sie zunächst die SafeGuard Enterprise Master-Datenbank an. In unserem Beispiel ist dies die Datenbank Wien.

Der Vorgang zum Erzeugen der Master-Datenbank ist mit dem entsprechenden Vorgang für eine SafeGuard Enterprise Installation ohne Replikation identisch.

- Erzeugen der Master-Datenbank im SafeGuard Management Center Konfigurationsassistenten.

  Für diesen Vorgang muss das SafeGuard Management Center bereits installiert sein. Für weitere Informationen *siehe Starten der Erstkonfiguration des SafeGuard Management Center* (Seite 35).

- Erzeugen der Master-Datenbank mit einem SQL Skript, das in der Produktlieferung Verfügung steht.

  Dieser Vorgang wird häufig bevorzugt, wenn erweiterte SQL-Berechtigungen während der SafeGuard Management Konfiguration nicht erwünscht sind. Für weitere Informationen *siehe Erzeugen der SafeGuard Enterprise Datenbank per Skript* (Seite 29).

14.2.2 Erzeugen der Replikationsdatenbanken Graz und Linz

Nach dem Einrichten der Master-Datenbank können Sie die Replikationsdatenbanken erzeugen. Im Beispiel haben die Replikationsdatenbanken die Bezeichnungen Graz und Linz.

Hinweis:

Datentabellen und EVENT-Tabellen werden in getrennten Datenbanken gehalten. Ereigniseinträge werden standardmäßig nicht verkettet, so dass die EVENT-Datenbank zur

Erhöhung der Performance auf mehrere SQL Server repliziert werden kann. Wenn EVENT-Tabellen verkettet werden, können während der Replikation ihrer Datensätze Probleme auftreten.

So erzeugen Sie die Replikationsdatenbanken neu:

1. Erzeugen Sie eine Veröffentlichung für die Master-Datenbank in der Managementkonsole des SQL Servers.

   Eine Veröffentlichung definiert das Daten-Set, das repliziert werden soll.
2. Wählen Sie alle Tabellen, Ansichten und gespeicherten Prozeduren für die Synchronisierung in dieser Veröffentlichung aus.
3. Erstellen Sie die Replikationsdatenbanken, indem Sie ein Abonnement für Graz und ein Abonnement für Linz erzeugen. Die neuen Datenbanken Graz und Linz erscheinen daraufhin in den Abonnements im SQL Konfigurationsassistenten.
4. Schließen Sie den SQL Konfigurationsassistenten. Die Replikationsüberwachung zeigt, ob der Replikationsmechanismus korrekt läuft.
5. Stellen Sie sicher, dass Sie den korrekten Datenbanknamen in der ersten Zeile des SQL Skripts eingeben. Verwenden Sie zum Beispiel **Graz** oder **Linz**.
6. Erzeugen Sie nochmal die Snapshots mit dem Snapshot Agenten.

Die Replikationsdatenbanken Graz und Linz wurden angelegt.

14.3 Installieren und Registrieren von SafeGuard Enterprise Servern

Um SafeGuard Enterprise Server auf den Web Servern zu installieren, gehen Sie wie folgt vor.

1. Installieren Sie SafeGuard Enterprise Server auf dem Server WS_1.
2. Installieren Sie SafeGuard Enterprise Server auf dem Server WS_2.
3. Registrieren Sie beide Server im SafeGuard Management Center. Klicken Sie im **Extras** Menü auf **Konfigurationspakete...** und dann auf **Server registrieren**. Klicken Sie in der Registerkarte **Server registrieren** auf **Hinzufügen**.
4. Sie werden dazu aufgefordert, die Serverzertifikate **ws_1.cer** und **ws_2.cer** hinzuzufügen. Sie finden die Zertifikate im Ordner **\Program Files\Sophos\SafeGuard Enterprise\MachCert**. Die Zertifikate werden benötigt, um die entsprechenden Konfigurationspakete zu erstellen.

Die SafeGuard Enterprise Server sind installiert und registriert.

14.4 Erzeugen der Konfigurationspakete für die Datenbank GRAZ

Erzeugen Sie die Konfigurationspakete für die Datenbank GRAZ: ein Paket für Server WS_1 für die Kommunikation mit der Datenbank GRAZ sowie ein Paket für die Verbindung des SafeGuard Enterprise Clients GRAZ mit dem Web Service WS_1.

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Optionen** und dann auf **Datenbank**.
2. Wählen Sie unter **Verbindungseinstellungen WS_1** als **Datenbankserver** und GRAZ als **Datenbank auf Server**. Klicken Sie auf **OK**.

3. Klicken Sie im **Extras** Menü auf **Konfigurationspakete...** und dann auf **Server-Konfigurationspaket erstellen**. Wählen Sie den Server **WS_1** , den Ausgabepfad und klicken Sie auf **Konfigurationspaket erstellen**.
4. Wechseln Sie auf die Registerkarte **Konfigurationspaket (Managed) erstellen**. Klicken Sie auf **Konfigurationspaket hinzufügen** und geben Sie einen Namen für das Paket ein. Wählen Sie unter **Primärer Server** den korrekten Server, mit dem die SafeGuard Enterprise Clients GRAZ verbunden werden sollen: **WS_1**. Legen Sie den Ausgabepfad fest und klicken Sie auf **Konfigurationspaket erstellen**.

Die SafeGuard Enterprise Server und Client Konfigurationspakete für die Datenbank GRAZ werden am definierten Ausgabeort erstellt.

14.5 Erzeugen der Konfigurationspakete für die Datenbank LINZ

Sie müssen die Konfigurationspakete für die Datenbank LINZ erzeugen: Ein Paket für Server WS_2 für die Kommunikation mit der Datenbank GRAZ sowie ein Paket für die Verbindung des SafeGuard Enterprise Clients LINZ mit dem Web Service WS_2.

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Optionen** und dann auf **Datenbank**.
2. Wählen Sie unter **Verbindungseinstellungen WS_2** als **Datenbankserver** und LINZ als **Datenbank auf Server**. Klicken Sie auf **OK**.
3. Klicken Sie im **Extras** Menü auf **Konfigurationspakete...** und dann auf **Server-Konfigurationspaket erstellen**. Wählen Sie den Server **WS_2** , den Ausgabepfad und klicken Sie auf **Konfigurationspaket erstellen**.
4. Wechseln Sie auf die Registerkarte **Konfigurationspaket (Managed) erstellen**. Klicken Sie auf **Konfigurationspaket hinzufügen** und geben Sie einen Namen für das Paket ein. Wählen Sie unter **Primärer Server** den korrekten Server, mit dem die SafeGuard Enterprise Clients LINZ verbunden werden sollen: **WS_2**. Legen Sie den Ausgabepfad fest und klicken Sie auf **Konfigurationspaket erstellen**. Klicken Sie auf **Schließen**.
5. Verbinden Sie das SafeGuard Management Center wieder mit der Datenbank WIEN: Klicken Sie im **Extras** Menü auf **Optionen** und dann auf **Datenbankverbindung**.

Die SafeGuard Enterprise Server und Client Konfigurationspakete für die Datenbank LINZ werden am definierten Ausgabeort erstellt.

14.6 Installieren der SafeGuard Enterprise Server Konfigurationspakete

1. Installieren Sie das Server-Konfigurationspaket (**ws_1.msi**) auf Web Service WS_1, der mit der Datenbank GRAZ kommunizieren soll.
2. Installieren Sie das Server-Konfigurationspaket **ws_2.msi** auf Web Service WS_2, der mit der Datenbank LINZ kommunizieren soll.
3. Testen Sie die Kommunikation zwischen den SafeGuard Enterprise Servern und diesen Datenbanken, *siehe Testen Der Verbindung (IIS 6 auf Windows Server 2003)* (Seite 47).

14.7 Installieren der SafeGuard Enterprise Client Software und der Konfiguration auf den Endpoint-Computern

Die Installation der SafeGuard Enterprise Client Software entspricht der Client-Installation ohne Replikation. Für weitere Informationen, *siehe Kommando für zentrale Installation* (Seite 64) .

Hinweis:

Stellen Sie für eine korrekte Konfiguration nach der Installation der einzelnen SafeGuard Enterprise Clients sicher, dass Sie das richtige Client-Konfigurationspaket installieren:

1. Installieren Sie das Client-Konfigurationspaket GRAZ auf den Clients, die mit dem GRAZ-Server WS_1 verbunden werden sollen.
2. Installieren Sie das Client-Konfigurationspaket LINZ auf den Clients, die mit dem LINZ-Server WS_2 verbunden werden sollen.

Für Informationen zur Aktualisierung von replizierten SafeGuard Enterprise Datenbanken, *siehe Aktualisieren von replizierten SafeGuard Enterprise Datenbanken* (Seite 90).

15 Aktualisieren von SafeGuard Enterprise

Wenn Sie bereits eine Vorgängerversion von SafeGuard Enterprise installiert haben, können Sie SafeGuard Enterprise durch die Installation der neuesten Version aktualisieren. Die Aktualisierung auf SafeGuard Enterprise Version 5.6x wird ab SafeGuard Enterprise Version 5.40 oder höher unterstützt. Für ältere Versionen müssen Sie zunächst eine Aktualisierung auf Version 5.40 durchführen.

Bis auf die SafeGuard Enterprise Datenbank handelt es sich bei der Aktualisierung des SafeGuard Enterprise Server, SafeGuard Management Center und SafeGuard Enterprise Client um Neuinstallationen.

Ab SafeGuard Enterprise 5.30 aufwärts ist der Import einer gültigen Lizenzdatei erforderlich, die alle ausgerollten SafeGuard Clients abdeckt. Wenn die Anzahl der Lizenzen überschritten ist, wird die Richtlinienübertragung nach der Aktualisierung des Backends blockiert. Bitte wenden Sie sich vor der Aktualisierung an Ihren Vertriebspartner und fordern Sie eine Lizenzdatei an.

Hinweis:

Halten Sie bei der Aktualisierung unbedingt die unten aufgeführte Reihenfolge ein. Nur dann ist eine Aktualisierung von einer früheren Version auf die aktuelle Version von SafeGuard Enterprise erfolgreich.

1. SafeGuard Enterprise Datenbank
2. SafeGuard Enterprise Server
3. SafeGuard Management Center
4. Durch SafeGuard Enterprise geschützte Endpoint-Computer

15.1 Aktualisieren der SafeGuard Enterprise Datenbank

Voraussetzungen

- SafeGuard Enterprise Datenbank 5.20 oder höher muss installiert sein.
- Die auszuführenden SQL-Skripts müssen auf dem Datenbank-Rechner vorhanden sein.
- Für die erfolgreiche Aktualisierung auf die aktuelle Version muss .NET Framework 3.0 Service Pack 1 installiert sein.
- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.
- Führen Sie ein Backup der Datenbank durch, bevor Sie mit der Aktualisierung beginnen.

Im Tools-Verzeichnis Ihrer Produktlieferung finden Sie mehrere SQL-Skripts für die Aktualisierung der Datenbank.

So aktualisieren Sie die Datenbank:

1. Nehmen Sie alle SafeGuard Enterprise Server (IIS Server) vom Netz, die mit der relevanten SafeGuard Enterprise Datenbank verbunden sind.
2. Schließen Sie das SafeGuard Management Center.
3. Stellen Sie zum Ausführen der Skripts die Datenbank auf den SINGLE_USER-Modus um, damit Sie exklusiven Zugriff auf die Datenbank haben.

4. Die Datenbank muss Version für Version auf die aktuelle Version konvertiert werden. Abhängig von der installierten Version, starten Sie nacheinander die folgenden SQL-Skripts:
   a) 5.20 > 5.3x: **MigrateSGN520_SGN530.sql** oder **MigrateSGN520_SGN535.sql** ausführen

      Vorhandene SafeGuard Enterprise Richtlinien werden modifiziert, da sich die Richtlinienstruktur von Version 5.20 zu 5.3x geändert hat.

   b) 5.3x > 5.35: **MigrateSGN530_SGN535.sql** ausführen
   c) 5.3x > 5.4x: **MigrateSGN530_SGN535.sql** ausführen
   d) 5.35 > 5.4x: **MigrateSGN535_SGN540.sql** ausführen
   e) 5.4x > 5.5x: **MigrateSGN540_SGN550.sql** ausführen
   f) 5.5x > 5.6x: **MigrateSGN550_SGN560.sql** ausführen
5. Stellen Sie die relevante Datenbank wieder auf den MULTI_USER-Modus zurück.

Nach Aktualisierung der Datenbank sind unter Umständen die kryptographischen Prüfsummen einiger Tabellen nicht mehr korrekt. Wenn Sie das SafeGuard Management Center starten, werden die entsprechenden Warnungsmeldungen angezeigt. Sie können die Tabellen dann in den entsprechenden Dialogen reparieren.

Die aktuelle Version der SafeGuard Enterprise Datenbank ist einsatzbereit.

Hinweis:

Im nächsten Schritt aktualisieren Sie das SafeGuard Management Center auf die aktuelle Version. Andernfalls wird eine Fehlermeldung angezeigt.

15.2 Aktualisieren von replizierten SafeGuard Enterprise Datenbanken

Wenn die SafeGuard Enterprise Datenbank zu einer neueren Version aktualisiert werden soll und replizierte Datenbanken verwendet werden, ist es am besten, die replizierten Datenbanken zu deinstallieren, bevor Sie mit der Aktualisierung der Master-Datenbank beginnen.

Für die Aktualisierung von SafeGuard Enterprise Datenbanken ist die Ausführung von speziellen SQL-Migrationsskripten erforderlich, die andernfalls einen Konflikt mit den replizierten Datenbanken auslösen können.

So aktualisieren Sie die replizierte Datenbank:

1. Deinstallieren Sie die replizierten Datenbanken.
2. Wenden Sie die SQL-Migrationsskripts auf die Master-Datenbank an. Sie finden die Skripts im Verzeichnis Tools in Ihrer Produktlieferung, *siehe Aktualisieren der SafeGuard Enterprise Datenbank* (Seite 89).
3. Richten Sie die replizierten Datenbanken neu ein, *siehe Replikation der SafeGuard Enterprise Datenbank* (Seite 84).

15.3 Aktualisieren des SafeGuard Enterprise Servers

Voraussetzungen

- SafeGuard Enterprise Server 5.35 oder höher muss installiert sein. Ältere Versionen als 5.35 müssen zunächst auf SafeGuard Enterprise Server 5.40 aktualisiert werden.
- .NET Framework 3.0 Service Pack 1 muss installiert sein. AP.NET 2.0 muss auf Version 2.0. aktualisiert sein.
- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.

So aktualisieren Sie den SafeGuard Enterprise Server:

1. Installieren Sie die neueste Version des SafeGuard Enterprise Server Installationspakets.

Der SafeGuard Enterprise Server ist aktualisiert. Er wird automatisch neu gestartet und kann benutzt werden.

15.4 Aktualisieren des SafeGuard Management Center

Voraussetzungen

- SafeGuard Management Center 5.40 oder eine neuere Version muss installiert sein. Ältere Versionen als 5.40 müssen zunächst auf SafeGuard Management Center 5.40 aktualisiert werden.
- Die Aktualisierung der SafeGuard Enterprise Datenbank und des SafeGuard Enterprise Servers auf die aktuelle Version wurde bereits durchgeführt.
- Die Aktualisierung der SafeGuard Enterprise Datenbank auf die aktuelle Version wurde bereits durchgeführt. Die Versionsnummer der SafeGuard Enterprise Datenbank und des SafeGuard Management Center müssen übereinstimmen.
- .NET Framework 3.0 Service Pack 1 muss installiert sein. ASP.NET muss auf Version 2.0. aktualisiert sein.
- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.
- Sie benötigen eine gültige Lizenzdatei. Wenden Sie sich dafür vorab an Ihren Vertriebspartner.

Hinweis:

Ist das SafeGuard Management Center auf einem Computer installiert, auf dem auch der SafeGuard Enterprise Client installiert ist, aktualisieren Sie die SafeGuard Enterprise Client Software zunächst auf Version 5.6x. Aktualisieren Sie dann das SafeGuard Management Center auf Version 5.6x. Wenn Sie nur das SafeGuard Management Center aktualisieren, kann dies zu fehlgeschlagenen Anmeldungen auf Windows-Ebene führen.

Nach der Aktualisierung des SafeGuard Management Centers auf Version 5.6x sollten POA-Benutzer nicht auf SafeGuard Enterprise Clients 5.4x oder 5.5x übertragen werden. Dies wird in diesem Fall nicht unterstützt, da der POA-Benutzer Besitzer des Computers werden würde.

So aktualisieren Sie das SafeGuard Management Center:

1. Installieren Sie die aktuelle Version des SafeGuard Management Center Installationspakets mit den erforderlichen Features, *siehe Einrichten des SafeGuard Management Centers* (Seite 33).
2. Importieren Sie die Lizenzdatei.
3. Starten Sie das SafeGuard Management Center. Das Systemverhalten beim ersten Start des SafeGuard Management Centers nach der Aktualisierung richtet sich nach den installierten Features:

Option	Beschreibung
Das Feature Multi Tenancy ist nicht installiert.	Sie werden aufgefordert, die SafeGuard Management Center Sicherheitsbeauftragten-Anmeldeinformationen einzugeben.
Das Feature Multi Tenancy ist neu installiert.	Der SafeGuard Management Center Konfigurationsassistent wird gestartet. Sie werden dazu aufgefordert, die zu verwendende Datenbank auszuwählen. Der Assistent schlägt standardmäßig eine bereits vorher verwendete Datenbank vor. Wählen Sie die gewünschte Datenbank aus und beenden Sie den Assistenten.
Das Feature Multi Tenancy wurde deinstalliert.	Die zuletzt benutzte Datenbankkonfiguration wird im SafeGuard Management Center verwendet.

Das SafeGuard Management Center wurde auf die neueste Version aktualisiert.

Hinweis:

- Scripting API: Die Standardkonfigurationsdatei wurde umbenannt und an einem anderen Ablageort gespeichert. Stellen Sie sicher, dass Sie Pfad und Dateinamen gemäß dem neuen Ablageort ändern, wenn Sie die folgende Methode mit dem Parameter **confFilePathName** verwenden: **AuthenticateOfficer (string OfficerName, string PinOrPassword, stringconfFilePathName**).
- Vorhandene SafeGuard Enterprise-Richtlinien haben sich eventuell geändert, da sich die Richtlinienstruktur von SafeGuard Enterprise ab Version 5.30 aufwärts geändert hat.

15.5 Aktualisieren von durch SafeGuard Enterprise geschützten Computern

Voraussetzungen

- SafeGuard Enterprise Client 5.40 oder höher muss installiert sein. Ältere Versionen müssen zunächst auf SafeGuard Enterprise Client 5.40 aktualisiert werden.

  SafeGuard Management Center 5.6x und SafeGuard Enterprise Server 5.6x können SafeGuard Enterprise Clients (managed und standalone) Version 5.40 oder höher verwalten.

Verschiedene Client-Versionen sollten nur während der Aktualisierung vorhanden sein. In der allgemeinen Anwendung sollte eine Mischung vermieden werden.

Hinweis:

Nach der Aktualisierung des SafeGuard Management Centers auf Version 5.6x sollten POA-Benutzer nicht auf SafeGuard Enterprise Clients 5.4x oder 5.5x übertragen werden. Dies wird in diesem Fall nicht unterstützt, da der POA-Benutzer Besitzer des Computers werden würde.

- Die Aktualisierung der SafeGuard Enterprise Datenbank, des SafeGuard Enterprise Servers und des SafeGuard Management Centers muss bereits durchgeführt worden sein.
- Ein SafeGuard Enterprise Client 5.6x kann nicht mit einem SafeGuard Enterprise Server unter Version 5.6x verbunden werden.
- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.

Dieser Abschnitt gilt sowohl für SafeGuard Enterprise Clients (managed) als auch Sophos SafeGuard Client (standalone).

So aktualisieren Sie durch SafeGuard Enterprise geschützte Computer:

1. Installieren Sie das vorbereitende MSI-Paket **SGxClientPreinstall.msi**, das den Endpoint-Computer mit den nötigen Voraussetzungen für eine erfolgreiche Installation der aktuellen Verschlüsselungssoftware ausstattet.
2. Installieren Sie das entsprechende Verschlüsselungssoftware-Installationspaket (*Client*.msi) Version für Version, bis die aktuelle Version erreicht ist, *siehe Zentrales Installieren der Verschlüsselungssoftware* (Seite 62) oder *siehe Lokales Installieren der Verschlüsselungssoftware* (Seite 73).

   Der Windows Installer erkennt, welche Features bereits installiert sind und installiert auch nur diese Features neu. Wenn die Power-on Authentication installiert ist, steht nach erfolgreicher Migration (Richtlinien, Schlüssel usw.) auch ein aktualisierter POA-Kernel zur Verfügung.

   Um mit der Aktualisierung neue Features zu installieren, wählen Sie eine Installation vom Typ **Angepasst** aus. Wählen Sie dann die neuen Features und die zu aktualisierenden Features. Bei einer nicht überwachten Installation, verwenden Sie die Eigenschaft ADDLOCAL = zur Auswahl der gewünschten Features (vorhandene und neue).
3. Wenn sich die Konfiguration des Endpoint-Computers z. B. durch geänderte Richtlinieneinstellungen geändert hat, erstellen Sie ein neues Konfigurationspaket.
4. Löschen Sie alle veralteten oder nicht mehr verwendeten Konfigurationspakete auf dem Endpoint-Computer aus Sicherheitsgründen.
5. Installieren Sie das Konfigurationspaket auf den relevanten Endpoint-Computern.

   Wenn Sie versuchen, ein älteres Konfigurationspaket über ein neues zu installieren, wird die Installation abgebrochen.

Der Endpoint-Computer wird mit der aktuellen Version der Verschlüsselungssoftware mit den ausgewählten Features aktualisiert.

Hinweis:

Benutzer, die importiert wurden, als nur SafeGuard Data Exchange installiert wurde, werden nicht automatisch in die Power-on Authentication importiert, wenn SafeGuard Device Encryption später installiert wird. In diesem Fall müssen Sie eine Benutzeraktualisierung auslösen, indem Sie z. B. dem Verzeichnisstamm vorübergehend einen Schlüssel zuweisen.

15.6 Ausstatten von Sophos SafeGuard Clients (standalone) mit volume-basierender Verschlüsselung

Um einen Sophos SafeGuard Client (standalone), auf dem nur das SafeGuard Data Exchange Module mit dateibasierender Verschlüsselung installiert ist, mit volume-basierender Verschlüsselung auszustatten, müssen Sie die folgenden Schritte ausführen. Diese Schritte sind notwendig, um eine korrekte und sichere Anmeldung an der Power-on Authentication zu gewährleisten.

1. Deinstallieren Sie das SafeGuard Data Exchange Installationspaket (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi).
2. Deinstallieren Sie das Konfigurationspaket.
3. Installieren Sie das SafeGuard Enterprise Device Encryption Installationspaket mit volume- und dateibasierender Verschlüsselung (SGNClient.msi/SGNClient_x64.msi). Wenn Sie dazu aufgefordert werden, wählen Sie die Features **Device Encryption** und **Data Exchange** und beenden Sie den Installationsassistenten.
4. Erstellen Sie ein neues Konfigurationspaket und installieren Sie es auf dem Computer.

Der Sophos SafeGuard Client (standalone) wurde mit volume-basierender Verschlüsselung ausgestattet.

Hinweis:

Die Schlüssel-Recovery-Datei sowie die lokalen Schlüssel, die während der Installation des Data Exchange Pakets erzeugt wurden, bleiben erhalten.

15.7 Migrieren von Sophos SafeGuard Client (standalone) auf SafeGuard Enterprise Client (managed)

Es besteht die Möglichkeit, einen Endpoint-Computer mit einer Sophos SafeGuard Client (standalone) Konfiguration auf eine SafeGuard Enterprise Client (managed) Konfiguration zu migrieren. Die Endpoint-Computer werden dann im SafeGuard Management Center zu Objekten, die verwaltet werden können und eine Verbindung zum SafeGuard Enterprise Server haben.

Voraussetzungen

- Führen Sie ein Backup des Endpoint-Computers durch, bevor Sie die Migration starten.
- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.

So migrieren Sie Sophos SafeGuard Client (standalone) auf SafeGuard Enterprise Client (managed):

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**. Um das Konfigurationspaket für den SafeGuard Enterprise Client (managed) zu erzeugen, klicken Sie auf **Konfigurationspaket erstellen**.
2. Weisen Sie dieses Paket dem Endpoint-Computer über eine Gruppenrichtlinie zu.

   Die Authentisierung ist deaktiviert, da die Benutzer-Computer-Zuordnung nicht migriert wird. Nach der Migration sind die Endpoint-Computer damit ungeschützt!
3. Starten Sie den Endpoint-Computer neu. Die erste Anmeldung erfolgt noch über Autologon. Neue Schlüssel und Zertifikate werden dem Benutzer zugewiesen.
4. Starten Sie den Computer nochmal neu. Melden Sie sich an der Power-on Authentication an. Die Computer werden erst nach dem zweiten Neustart geschützt.
5. Löschen Sie veraltete und nicht mehr verwendete Konfigurationspakete.

Der Sophos SafeGuard Client (standalone) ist nun ein SafeGuard Enterprise Client (managed).

15.8 Aktualisieren des SafeGuard Configuration Protection Client

Für Informationen zum Aktualisieren des SafeGuard Configuration Protection Client Moduls, *siehe Aktualisieren von SafeGuard Configuration Protection* (Seite 83).

16 Aktualisieren des Betriebssystems

Wenn SafeGuard Enterprise installiert ist, ist es nur möglich, die Service Pack Version Ihres Betriebssystems zu aktualisieren.

Sie können z. B. ein neues Windows XP Service Pack installieren. Es ist jedoch nicht möglich, von einer Betriebssystem-Serie auf eine andere zu migrieren. Sie können z. B. nicht von Windows Vista auf Windows 7 umstellen, wenn SafeGuard Enterprise installiert ist.

17 Migration von Sophos SafeGuard auf SafeGuard Enterprise

Sophos SafeGuard lässt sich leicht auf die SafeGuard Enterprise Suite mit zentralem Management erweitern, um den vollen Funktionsumfang von SafeGuard Enterprise (z. B. Benutzer- und Computerverwaltung, umfangreiche Protokolldatei usw.) nutzen zu können.

Sophos SafeGuard umfasst die folgenden Produkte:

- Sophos SafeGuard Disk Encryption, welches mit ESDP (Endpoint Security and Data Protection) verfügbar ist.
- SafeGuard Easy: Ab Version 5.50 ist SafeGuard Easy der neue Produktname für die SafeGuard Enterprise Standalone-Lösung.

Die Migration umfasst folgende Schritte:

- Der SafeGuard Policy Editor muss auf das SafeGuard Management Center migriert werden.
- Durch Sophos SafeGuard (standalone) geschützte Endpoint-Computer müssen mit einer SafeGuard Enterprise (managed) Konfiguration ausgestattet werden.

17.1 Migration von SafeGuard Policy Editor auf SafeGuard Management Center

Voraussetzungen

- Sie müssen den SafeGuard Policy Editor nicht deinstallieren.
- Der SafeGuard Enterprise Server muss installiert und auf die aktuelle Version aktualisiert sein.
- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.

Für die Migration installieren Sie einfach das SGNManagementCenter.msi Paket auf dem Computer, auf dem der SafeGuard Policy Editor eingerichtet ist.

1. Starten Sie SGNManangementCenter.msi aus dem Installationsordner Ihrer Produktlieferung. Ein Assistent führt Sie durch die notwendigen Schritte.
2. Bestätigen Sie die **Willkommen** Seite und klicken Sie auf **Weiter**.
3. Akzeptieren Sie die Lizenzvereinbarung.
4. Übernehmen Sie den Standardinstallationspfad.
5. Wählen Sie den Installationstyp aus:
   - Wenn das SafeGuard Management Center für die Unterstützung von nur einer Datenbank installiert werden soll, wählen Sie eine Installation vom Typ **Typisch** aus.
   - Wenn das SafeGuard Management Center für die Unterstützung mehrerer Datenbanken installiert werden soll (**Multi Tenancy**), wählen Sie eine Installation vom Typ **Typisch** aus. Für weitere Informationen, *siehe Multi Tenancy Konfigurationen* (Seite 35).
6. Klicken Sie auf **Beenden**, um die Installation abzuschließen.
7. Starten Sie Ihren ggf. Computer neu.

8. Starten Sie das SafeGuard Management Center, um die Erstkonfiguration durchzuführen, *siehe Konfigurieren des SafeGuard Management Centers* (Seite 34).

Der SafeGuard Policy Editor wurde auf das SafeGuard Management Center migriert.

17.2 Migrieren von Sophos SafeGuard Client (standalone) auf SafeGuard Enterprise Client (managed)

Es besteht die Möglichkeit, einen Endpoint-Computer mit einer Sophos SafeGuard Client (standalone) Konfiguration auf eine SafeGuard Enterprise Client (managed) Konfiguration zu migrieren. Die Endpoint-Computer werden dann im SafeGuard Management Center zu Objekten, die verwaltet werden können und eine Verbindung zum SafeGuard Enterprise Server haben.

Voraussetzungen

- Führen Sie ein Backup des Endpoint-Computers durch, bevor Sie die Migration starten.
- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.

So migrieren Sie Sophos SafeGuard Client (standalone) auf SafeGuard Enterprise Client (managed):

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**. Um das Konfigurationspaket für den SafeGuard Enterprise Client (managed) zu erzeugen, klicken Sie auf **Konfigurationspaket erstellen**.
2. Weisen Sie dieses Paket dem Endpoint-Computer über eine Gruppenrichtlinie zu.

   Die Authentisierung ist deaktiviert, da die Benutzer-Computer-Zuordnung nicht migriert wird. Nach der Migration sind die Endpoint-Computer damit ungeschützt!
3. Starten Sie den Endpoint-Computer neu. Die erste Anmeldung erfolgt noch über Autologon. Neue Schlüssel und Zertifikate werden dem Benutzer zugewiesen.
4. Starten Sie den Computer nochmal neu. Melden Sie sich an der Power-on Authentication an. Die Computer werden erst nach dem zweiten Neustart geschützt.
5. Löschen Sie veraltete und nicht mehr verwendete Konfigurationspakete.

Der Sophos SafeGuard Client (standalone) ist nun ein SafeGuard Enterprise Client (managed).

18 Migration von SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x auf Sophos SafeGuard 5.6x

SafeGuard Easy (SGE) Version 4.5x sowie Sophos SafeGuard Disk Encryption Version 4.6x können direkt auf SafeGuard Enterprise 5.6x migriert werden, indem einfach das SafeGuard Enterprise Client Installationspaket auf dem Computer installiert wird.

Die Verschlüsselung von Festplatten bleibt bestehen. Diese müssen nicht entschlüsselt und neu verschlüsselt werden. SafeGuard Easy oder Sophos SafeGuard Disk Encryption muss auch nicht manuell deinstalliert werden.

Dieses Kapitel beschreibt, wie Sie eine Migration auf Sophos SafeGuard durchführen und zeigt, welche Features migriert werden können und welche Einschränkungen bestehen.

18.1 Voraussetzungen

- Die direkte Migration wurde getestet und wird unterstützt für SafeGuard Easy ab Version 4.5x. Eine direkte Migration sollte auch für Versionen zwischen 4.3x und 4.4x funktionieren.

  Für ältere Versionen wird die direkte Migration nicht unterstützt. Versionen vor 4.3x müssen daher zunächst auf SafeGuard Easy 4.50 aktualisiert werden.
- Die direkte Migration wird unterstützt für Sophos SafeGuard Disk Encryption 4.6x.
- SafeGuard Easy/Sophos SafeGuard Disk Encryption muss auf folgendem Windows Betriebssystem laufen:

  Windows XP Professional Workstation Service Pack 2, 3
- Windows Installer Version 3.01 oder höher muss installiert sein.
- Die Hardware muss mit den Systemvoraussetzungen für SafeGuard Enterprise 5.6x übereinstimmen.
- Wenn Sie spezifische Software (z. B. Lenovo-Middleware) verwenden, so muss diese mit den Systemvoraussetzungen für SafeGuard Enterprise 5.6x übereinstimmen.
- Festplatten müssen mit den folgenden Algorithmen verschlüsselt sein, um migriert werden zu können: AES128, AES256, 3DES, IDEA.
- Benutzer benötigen ein gültiges Windows-Konto und ein Kennwort. Falls der Benutzer sein Windows-Kennwort nicht weiß, weil er Secure Automatic Logon für die Windows-Anmeldung verwendet, muss das Windows-Kennwort des Benutzers zurückgesetzt werden. Das neue Kennwort muss dem Benutzer mitgeteilt werden. Für weitere Informationen *siehe Vorbereiten der Migration* (Seite 102).

18.2 Einschränkungen

- Es kann nur das SafeGuard Device Encryption Installationspaket mit dem Standard-Funktionsumfang installiert werden (SGNClient.msi). Wenn zusätzlich das Modul SafeGuard Data Exchange (SGNClient_withoutDE.msi) installiert werden soll,

muss dies in einem separaten Schritt erfolgen, da eine direkte Migration für dieses Paket nicht unterstützt wird.

- Folgende SafeGuard Easy Installationen können nicht auf SafeGuard Enterprise migriert werden. In diesen Fällen sollten Sie nicht versuchen, SafeGuard Enterprise zu installieren.

  Hinweis:

  Wenn Sie in den nachfolgend genannten Fällen eine Migration vornehmen, erhalten Sie eine Fehlermeldung (Fehlernummer 5006).

  Twin Boot Installationen
  Installationen mit aktivem Compaq Switch
  Lenovo Computrace Installationen
  Festplatten, die nur teilweise verschlüsselt sind, z. B. nur mit Verschlüsselung des Boot-Sektors.
  Festplatten mit versteckten Partitionen
  Festplatten, die mit einem der folgenden Algorithmen verschlüsselt sind: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16
  Multi-Boot Szenarien mit einer zweiten Windows- oder Linux-Partition

- Wechselmedien, die mit einem der folgenden Algorithmen verschlüsselt sind, können nicht migriert werden: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16.

  Hinweis:

  Es besteht die Gefahr von Datenverlust, wenn ein Wechselmedium mit einem der Algorithmen XOR, STEALTH, DES, RIJANDAEL, Blowfish-8, Blowfish-16 verschlüsselt wurde. Die Daten auf dem Wechselmedium können nach der Migration mit Sophos SafeGuard nicht mehr gelesen werden!

- Wechselmedien mit Super Floppy-Volumen können nach der Migration nicht umgewandelt werden.
- Wechselmedien können in das SafeGuard Enterprise Format konvertiert werden. Nach der Konvertierung kann ein verschlüsselter Datenträger nur noch mit SafeGuard Enterprise und nur auf dem Endpoint-Computer gelesen werden, an dem die Konvertierung durchgeführt wurde.

18.3 Welche Funktionalität wird migriert

Die folgende Tabelle zeigt, welche Funktionalität migriert wird und wie diese in SafeGuard Enterprise abgebildet wird.

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Upgrade	SafeGuard Enterprise
Verschlüsselte Festplatten	Ja	Die Festplattenschlüssel werden durch die SafeGuard Enterprise Power-on Authentication geschützt. Der Festplattenschlüssel ist somit zu keiner Zeit exponiert. Wenn der Modus "Boot

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Upgrade	SafeGuard Enterprise
		Protection" gewählt wurde, muss die bisherige SafeGuard Easy Version deinstalliert werden. Der Verschlüsselungsalgorithmus der Festplatte wird bei der Migration nicht verändert. Daher kann sich der tatsächliche Algorithmus einer solchen migrierten Festplatte von der allgemeinen SafeGuard Enterprise Richtlinie unterscheiden.
Verschlüsselte Wechselmedien (gilt nur für die Migration von SafeGuard Easy)	Ja	Verschlüsselte Datenträger, z. B. USB Flash Drive, können in das SafeGuard Enterprise Format konvertiert werden. **Hinweis:** Nach der Konvertierung kann ein verschlüsselter Datenträger nur noch mit SafeGuard Enterprise und nur auf dem Endpoint-Computer gelesen werden, an dem die Konvertierung durchgeführt wurde. Die Konvertierung muss jeweils bestätigt werden.
Verschlüsselungsalgorithmen	Teilweise	Die für die Migration geeigneten Algorithmen AES128, AES256, 3DES, IDEA werden migriert. AES-128 und 3-DES stehen jedoch nicht im Management Center zur Auswahl für neu zu verschlüsselnde Medien zur Verfügung.
Challenge/Response	Teilweise	Das Challenge/Response-Verfahren bleibt erhalten.
Benutzernamen	Nein	Da in SafeGuard Enterprise die Windows-Benutzernamen verwendet werden, ist eine Übernahme der bestehenden SafeGuard Easy/Sophos SafeGuard Disk Encryption Benutzernamen nicht nötig. Die Registrierung der migrierten Computer erfolgt deshalb wie bei einer Neuinstallation von SafeGuard Enterprise: durch zentrales Zuweisen oder lokales Registrieren der Computer-Benutzer. **Hinweis:** Nach der Migration wird der erste Benutzer, der sich an Windows anmeldet, als primärer Benutzer innerhalb der POA definiert (es sei denn, der Benutzer ist auf einer Service Account Liste aufgeführt).
Benutzerkennwörter	Nein	Da die Windows Kennwörter in SafeGuard Enterprise verwendet werden, müssen die SafeGuard Easy/Sophos SafeGuard Disk Encryption Kennwörter nicht übernommen werden. Die spezifischen SafeGuard Easy/Sophos SafeGuard Disk Encryption Kennwörter werden deshalb nicht migriert.

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Upgrade	SafeGuard Enterprise
Richtlinien, Einstellungen (z. B. Mindestpasswortlänge)	Nein	Zur Sicherstellung der Konsistenz der gesamten Einstellungen ist eine automatische Übernahme nicht vorgesehen. Die Einstellungen müssen im SafeGuard Management Center neu gesetzt werden.
Pre-Boot Authentisierung	Nein	Die Pre-Boot Authentication (PBA) wird durch die Sophos SafeGuard Power-on Authentication (POA) ersetzt.
Installationen ohne GINA	Ja	Installationen ohne GINA werden auf SafeGuard Enterprise mit installierter SGNGINA migriert.
Token/Smartcards (gilt nur für die Migration von SafeGuard Easy)	Teilweise	Die Token/Smartcard-Hardware kann in SafeGuard Enterprise weiterverwendet werden. Allerdings werden die Anmeldeinformationen nicht migriert. Die in SafeGuard Easy verwendeten Token müssen deshalb in SafeGuard Enterprise neu ausgestellt werden und wie bei jedem anderen SafeGuard Enterprise Endpoint-Computer über Richtlinien eingerichtet werden. SafeGuard Easy Anmeldeinformationen in Dateiform auf Token/Smartcards, bleiben als solche erhalten, können aber lediglich zur Anmeldung an Computern mit SafeGuard Easy Unterstützung verwendet werden. Falls notwendig, muss die benutzte Token/Smartcard-Middleware auf eine von SafeGuard Enterprise unterstützte Version aktualisiert werden.
Anmeldung mit Lenovo Fingerabdruck-Leser	Teilweise	Die Anmeldung per Fingerabdruck kann in SafeGuard Enterprise weiterhin benutzt werden. Die Hardware sowie die Software für den Fingerabdruck-Leser muss von SafeGuard Enterprise unterstützt werden. Außerdem müssen die Benutzerdaten erneut ausgerollt werden. Weitere Informationen zur Anmeldung per Fingerabdruck finden Sie in der Benutzerhilfe. Weitere Informationen zur Anmeldung per Fingerabdruck finden Sie in der Benutzerhilfe.

18.4 Vorbereiten der Migration

- Erstellen Sie zum Schutz vor Datenverlust ein komplettes Backup der zu migrierenden Computer.

  Führen Sie die vor der Installation der Verschlüsselungssoftware empfohlenen Schritte aus. Benutzen Sie z. B. **chkdsk** und **defrag**. Für weitere Informationen, *siehe Vorbereiten der Verschlüsselung* (Seite 57). Siehe auch:

chdsk: *http://www.sophos.de/support/knowledgebase/article/107799.html*.
defrag: *http://www.sophos.de/support/knowledgebase/article/109226.html*.

- Wir empfehlen, einen gültigen Kernel-Backup zu erstellen und diesen an einem Speicherort abzulegen, auf den immer zugegriffen werden kann (zum Beispiel Netzwerkpfad). Weitere Informationen hierzu finden Sie in den SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.6x Handbüchern/Hilfen im Kapitel *Systemkern sichern und Notfallmedien erstellen*.
- Legen Sie bei der ersten Migration zur Sicherheit eine Testumgebung an.
- Migrieren Sie ältere Versionen von SafeGuard Easy zuerst auf die Version 4.50.
- Lassen Sie die Computer während des gesamten Migrationsprozesses eingeschaltet.
- Der Sicherheitsbeauftragte sollte die Windows-Anmeldeinformationen der Benutzer bereithalten, falls diese nach der erfolgreichen Migration ihre Windows-Kennwörter vergessen haben. Dieser Fall kann eintreten, wenn die Benutzer sich früher an der Pre-Boot Authentisierung angemeldet haben und eventuell zu einem späteren Zeitpunkt über das Windows Secure Autologon (SAL) angemeldet wurden. Die Benutzer haben somit nie ihre Windows-Anmeldeinformationen benutzt.

  Hinweis:

  Benutzern muss vor der Migration ein Kennwort zur Windows-Anmeldung bekannt sein. Dies ist wichtig, da ein Windows-Kennwort nicht nachträglich nach der Migration und Installation von SafeGuard Enterprise gesetzt werden kann. Wenn die Benutzer Ihr Windows-Kennwort nicht kennen, weil Sie sich über SAL in SafeGuard Easy/Sophos SafeGuard Disk Encryption angemeldet haben, können sie sich an SafeGuard Enterprise nicht anmelden. Die automatische Anmeldung an Windows wird in diesem Fall abgewiesen und die Benutzer können sich nicht mehr an SafeGuard Enterprise anmelden. Es besteht die Gefahr des Datenverlusts, da Benutzer nicht in der Lage sind, auf ihre Computer zuzugreifen.

18.5 Starten der Migration

Hinweis:

Die Installation kann auf einem laufenden SafeGuard Easy/Sophos SafeGuard Disk Encryption System durchgeführt werden. Verschlüsselte Festplatten oder Volumes müssen nicht vorab entschlüsselt werden.

Verwenden Sie das SafeGuard Device Encryption Client Installationspaket (SGNClient.msi) aus dem Installationsverzeichnis mit dem Standard-Funktionsumfang. Das Client-Paket SGNClient_withoutDE.msi kann nicht verwendet werden. Die Installation sollte am besten zentral im unbeaufsichtigten Modus erfolgen. Die lokale Installation über das Setup-Verzeichnis wird nicht empfohlen!

So führen Sie die Migration durch:

1. Doppelklicken Sie im SafeGuard Easy/Sophos SafeGuard Disk Encryption Programmordner des zu migrierenden Endpoint-Computers auf WIZLDR.exe. Der Migrationsassistent wird gestartet.

2. Geben Sie im Migrationsassistenten das SYSTEM-Kennwort ein und klicken Sie auf **Weiter**. Klicken Sie im **Zielordner** auf **Weiter** und dann auf **Beenden**. Die Migrations-Konfigurationsdatei **SGEMIG.cfg** wird erzeugt.
3. Benennen Sie diese Datei im Windows Explorer von **SGEMIG.cfg** in **SGE2SGN.cfg** um.

   Hinweis: "Ersteller/Besitzer"-Rechte müssen für diese Datei und den Dateipfad gesetzt sein, auf dem sie während der Migration gespeichert ist. Andernfalls schlägt die Migration fehl und eine Meldung wird ausgegeben, dass **SGE2SGN.cfg** nicht gefunden werden konnte.
4. Geben Sie das Kommando **msiexec** in der Eingabeaufforderung ein, um das vorbereitende SafeGuard Enterprise Installationspaket sowie das SafeGuard Enterprise Device Encryption Client Installationspaket auf dem SafeGuard Easy/Sophos SafeGuard Disk Encryption Computer zu installieren. Fügen Sie den Parameter MIGFILE mit dem Pfad der Migrationsdatei **SGE2SGN.cfg** hinzu.

   Beispiel:

   msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SGxClientPreinstall.msi

   msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SGNClient.msi

   /L*VX“\\Distributionserver\Software\Sophos\SafeGuard\%Computername%.log“

   MIGFILE=\\Distributionserver\Software\Sophos\SafeGuard\SGE2SGN.cfg

- Wenn die Migration erfolgreich durchgeführt wurde, kann SafeGuard Enterprise auf dem Computer benutzt werden.
- Schlägt die Migration fehl, kann SafeGuard Easy/Sophos SafeGuard Disk Encryption immer noch auf dem Computer benutzt werden. In diesem Fall wird SafeGuard Enterprise automatisch entfernt.

18.6 Anmelden am Endpoint-Computer nach der Migration

So melden Sie sich an einem Computer an, der von SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.6x auf SafeGuard Enterprise 5.6x migriert wurde:

1. Starten Sie den migrierten Endpoint-Computer neu. Die erste Anmeldung erfolgt noch über Autologon. Neue Schlüssel und Zertifikate werden dem Benutzer zugewiesen.
2. Starten Sie den Computer nochmal neu. Melden Sie sich an der Power-on Authentication an. Die Computer werden erst nach dem zweiten Neustart geschützt.
3. Um in der Lage zu sein, die Festplatte zu entschlüsseln und Schlüssel für die Festplattenverschlüsselung hinzuzufügen und zu entfernen, starten Sie den Computer noch einmal neu.

Nach erfolgreicher Migration steht Ihnen in SafeGuard Enterprise nach der Anmeldung an der Power-on Authentication folgendes zur Verfügung:

- die Schlüssel und Algorithmen der verschlüsselten Festplatten

  Verschlüsselte Volumes bleiben verschlüsselt und die Verschlüsselungschlüssel werden automatisch in ein SafeGuard Enterprise kompatibles Format konvertiert.

- die Schlüssel und Algorithmen für verschlüsselte Wechselmedien (nur bei Migration von SafeGuard Easy).

  Wechselmedien müssen in ein SafeGuard Enterprise kompatibles Format konvertiert werden.

18.7 Konfigurieren von migrierten Endpoint-Computern

Endpoint-Computer werden initial über Konfigurationspakete konfiguriert, die zum Beispiel die Power-on Authentication aktivieren.

Voraussetzungen:

Die Konfiguration der Endpoint-Computers sollte erst nach der Migration sowie nach der Aktivierung der POA und der erfolgreichen Anmeldung des Benutzers an Windows auf dem migrierten Computer durchgeführt werden.

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete** und erstellen Sie das erste Konfigurationspaket mit den erforderlichen Richtlinieneinstellungen.

   Die mit dem ersten Konfigurationspaket übertragenen Richtlinien sollten mit der vorigen Konfiguration des SafeGuard Easy/Sophos SafeGuard Disk Encryption Computers übereinstimmen.

   Wenn nach der Migration kein Konfigurationspaket installiert wird, bleiben alle Laufwerke, die mit SafeGuard Easy/Sophos SafeGuard Disk Encryption verschlüsselt wurden, verschlüsselt.
2. Installieren Sie das Konfigurationspaket auf den Endpoint-Computern.

18.8 Konvertieren von Schlüsseln für verschlüsselte Wechselmedien

Um die Umwandlung überhaupt erst zu initiieren, muss auf dem Computer die entsprechende Richtlinie für volume-basierende Verschlüsselung vorliegen. Andernfalls werden die Schlüssel nicht konvertiert.

Verschlüsselte Wechselmedien bleiben ebenfalls verschlüsselt, müssen aber in ein SafeGuard Enterprise kompatibles Schlüsselformat umgewandelt werden.

Hinweis:

Deshalb kann ein verschlüsseltes Wechselmedium nach der Konvertierung nur mit SafeGuard Enterprise gelesen werden und nur an dem Endpoint-Computer, an dem es während der Migration konvertiert wurde!

1. Nehmen Sie das Wechselmedium vom Computer ab und verbinden Sie es danach wieder mit dem Computer. Somit stellen Sie sicher, dass Sie Wechselmedien entschlüsseln oder Schlüssel für die Verschlüsselung von Wechselmedien hinzufügen und entfernen können.
2. Klicken Sie im Windows Explorer auf das Wechselmedium doppelt, auf das Sie zugreifen möchten.

3. Sie werden dazu aufgefordert, die Umwandlung der Verschlüsselungsschlüssel in ein SafeGuard Enterprise kompatibles Format zu bestätigen.
   - Wenn Sie die Umwandlung bestätigen, so ist der Zugriff auf die migrierten Daten in vollem Umfang möglich.
   - Wenn Sie die Umwandlung ablehnen, lassen sich die migrierten Daten noch zum Lesen und Schreiben öffnen.

Neu hinzukommende Wechselmedien werden wie bei jedem SafeGuard Enterprise Computer verschlüsselt, wenn die entsprechende Richtlinie am Endpoint-Computer vorliegt.

19 Deinstallation - Überblick

- Wenn die SafeGuard Enterprise Verschlüsselungssoftware auf demselben Computer wie das SafeGuard Management Center, SafeGuard Enterprise Server oder SafeGuard Web Help Desk installiert ist, führen Sie den folgende Deinstallationsvorgang durch, damit Sie weiterhin eine der Komponenten benutzen können:
    1. Deinstallieren Sie das SafeGuard Management Center, SafeGuard Enterprise Server oder SafeGuard Web Help Desk.
    2. Deinstallieren Sie das SafeGuard Enterprise Client Konfigurationspaket.
    3. Deinstallieren Sie die SafeGuard Enterprise Client Verschlüsselungssoftware.
    4. Installieren Sie das Paket, das Sie weiterhin benutzen möchten, neu. Um das SafeGuard Management Center benutzen zu können, importieren Sie nach der Installation das alte Maschinenzertifikat. Um die SafeGuard Enterprise Verschlüsselungssoftware benutzen zu können, installieren Sie nach der Installation der Verschlüsselungssoftware das Client Konfigurationspaket.
- Bevor Sie die Verschlüsselungssoftware deinstallieren, deinstallieren Sie zunächst das Konfigurationspaket.
- Sie können die Verschlüsselungssoftware für Volumes, die mit einem benutzerspezifischen Schlüssel verschlüsselt sind, der Ihnen nicht zugewiesen ist, nicht deinstallieren.
- Wenn Sie SafeGuard Device Encryption Client Volumes deinstallieren, die mit dem Standard-Maschinenschlüssel verschlüsselt wurden, werden diese automatisch entschlüsselt. Um mit anderen Schlüsseln verschlüsselte Volumes zu entschlüsseln, erstellen Sie vor der Deinstallation von SafeGuard Device Encryption eine entsprechende Richtlinie und weisen Sie diese zu.
- Während der Deinstallation der Verschlüsselungssoftware, die auch die Entschlüsselung verschlüsselter Volumes umfasst, sollte der Computer nicht heruntergefahren oder neu gestartet werden. Andernfalls gibt der Deinstaller eine Fehlermeldung aus.
- Wird die Deinstallation über ein Active Directory ausgelöst, stellen Sie sicher, dass zuvor alle volume-basierend verschlüsselten Volumes korrekt entschlüsselt wurden.
- Nach einer Deinstallation verbleiben u. U. einige Dateien und Registry-Einträge auf dem Computer. Informationen zur manuellen Säuberung der Installation finden Sie in der Sophos Wissensdatenbank (Stichwörter “SGN & uninstall”). Eine manuelle Säuberung ist notwendig, damit die Verschlüsselungssoftware auf dem Computer erneut erfolgreich installiert werden kann.
- Wenn Sie SafeGuard Device Encryption und SafeGuard Data Exchange auf einem Computer installiert haben, können Sie SafeGuard Device Encryption nicht separat deinstallieren. Sie müssen das komplette Paket deinstallieren.
- Bevor Sie eine Deinstallation des letzten SafeGuard Enterprise Client, auf den Zugriff besteht, durchführen, sollten Sie alle verschlüsselten Wechselmedien entschlüsseln. Andernfalls besteht die Gefahr, dass Sie nicht mehr auf Ihre Daten zugreifen können. Solange Sie Ihre SafeGuard Enterprise Datenbank beibehalten, können die Daten auf den Wechselmedien wiederhergestellt werden.

19.1 Verhindern der Deinstallation auf Endpoint-Computern

Um Endpoint-Computer zusätzlich zu schützen, kann die lokale Deinstallation von Sophos SafeGuard verhindert werden. Setzen Sie das Feld **Deinstallation erlaubt** in einer **Spezifische Computereinstellungen** Richtlinie auf **Nein** und übermitteln Sie die Richtlinie an die Endpoint-Computer. Nach Wirksamwerden einer solchen Richtlinie auf dem Endpoint-Computer werden Deinstallationsvorgänge abgebrochen. Jeder unautorisierte Deinstallationsversuch wird protokolliert.

Hinweis:

Wenn Sie eine Demoversion verwenden, sollten Sie diese Richtlinieneinstellung nicht aktivieren bzw. vor Ablauf der Demoversion deaktivieren, damit die Demoversion auf einfache Art und Weise deinstalliert werden kann.

20 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter *http://community.sophos.com/* auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter *http://www.sophos.de/support/*.
- Laden Sie Dokumentation zu den Produkten unter *http://www.sophos.de/support/docs/* herunter.
- Senden Sie eine E-Mail an den technischen Support *support@sophos.de* und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

21 Rechtliche Hinweise